International Journal of Safety and Security Engineering
Vol. 16, No. 4, April, 2026, pp. 761-773
Journal homepage: http://iieta.org/journals/ijsse

Between Compliance and Illusion: A Comparative Study of Cookie Consent Mechanisms Across Regulatory Frameworks

Malak Ourrahte*, Fatima-Ezzahra Ziani, Ahmed El-Yahyaoui

Intelligent Processing and Security of Systems (IPSS), Faculty of Sciences, Mohammed V University, Rabat 10000, Morocco

Corresponding Author Email: malak_ourrahte@um5.ac.ma

https://doi.org/10.18280/ijsse.160406

Received: 14 February 2026
Revised: 5 April 2026
Accepted: 24 April 2026
Available online: 30 April 2026

Keywords:
cookie banners, consent, data protection, legal compliance, privacy, user choice, user tracking, web cookies

ABSTRACT

Cookie consent mechanisms are widely used to implement data protection policies on the Internet. However, the level of compliance among websites remains highly variable and insufficiently assessed in international comparisons. This article presents an empirical study of consent collection practices in five countries with different regulatory frameworks: France, Germany, Japan, the United States, and Morocco. A dataset of 1,000 websites covering five sectors (media, e-commerce, health, education, and government) was analyzed using an automated protocol based on Playwright. To quantify website compliance with regulatory requirements, we developed a synthetic indicator, the Cookie Compliance Score (CCS). This indicator measures the presence of consent banners, explicit choices to accept or reject all cookies, the absence of pre-checked boxes, and even the limitation of third-party cookies prior to consent. The study was also enriched by the capture of questionable design situations (dark patterns). The results show significant differences between countries. EU member states generally have the highest compliance rates while third countries have far lower scores. Interestingly, these higher levels of formal compliance are often associated with a stronger presence of dark patterns. These findings highlight both the importance and the limitations of current regulatory frameworks for effective user consent.

1. INTRODUCTION

Over the past decade, concerns about for protecting online user data have become one of the primary issues facing the modern web. With the widespread use of digital services, internet browsing has become a valuable resource for businesses. At the same time, users have become aware of the monitoring and analysis of their online habits and interactions. These are carried out for advertising or commercial purposes [1].

Cookies are one of the most popular tracking techniques. Cookies are very small files of data that get saved on a person's browser when they go to a website. Primarily, these cookies are utilized for tracking and viewing the online behavior of users and also for recognizing their likes and preferences [2]. However, their use raises fundamental questions about privacy.

To combat these techniques, several legal frameworks have been established with the aim of maintaining and restoring user control over their data, such as the General Data Protection Regulation (GDPR) in The European Union [3], which imposes strict obligations on companies that utilize them. This has led to the widespread use of cookie banners on websites to obtain users' consent before collecting any data. Other countries, such as the United States, Japan, and Morocco, have also implemented regulations such as the California Consumer Privacy Act (CCPA) [4], Act on the Protection of Personal Information (APPI) [5], and Law 09-08 [6], to regulate the collection of personal data, but these have been applied in different ways.

Based on all of the above, the application of these regulations gives users the option to refuse or accept the trackers used by websites. But in reality, are these regulations truly effective? Is the user's choice technically respected? Does simply displaying a banner mean that data is not collected without consent? And most importantly, is this protection equivalent from one country to another [7]?

Many recent studies have shown that websites often fail to respect users' choices. Some sites place cookies even before the user can take any action, and marketing or analytics cookies are retained even if a user has clearly refused them. What's more, some cookie banners use misleading designs, with easily accessible accept buttons, while access to the decline button is hidden or complicated, which is referred to as “dark patterns” [8].

In this context, the aim of this research is to examine, through an empirical and technical study, the effectiveness of cookie consent mechanisms within different legislative frameworks. The main research question addressed in this article is as follows: To what extent do cookie consent mechanisms actually implement users’ choices from a technical standpoint in different countries? To answer this question, the study is structured around the following sub-questions:

• What are the cookie consent mechanisms in different jurisdictions?

• To what extent are users' choices technically respected before and after interacting with the banner?

• Are there significant differences in terms of compliance and design practices between countries?

• How do interface design strategies, including dark patterns, influence user consent?

To answer these questions, we are conducting an empirical study comparing cookie consent procedures across five jurisdictions: France, Germany, the United States, Japan, and Morocco. Rather than quantifying legal compliance in the strict sense, this study focuses on the gap between authorized consent and the actual tracking practices observed on-site. This assessment is based on automated technical measurements, taking into account the placement of cookies before and after the user's visit, the collection of third-party trackers, and the use of "dark patterns".

To summarize these observations, we introduce the Cookie Compliance Score (CCS), a discrete metric that incorporates several technical and ergonomic criteria related to preserving the integrity of consent mechanisms. The CCS is never intended to directly assess the legal compliance of websites, but to provide a comparable indicator of the effective quality of consent offered to users.

We have made a threefold contribution. First, we propose an automated and reproducible measurement protocol that allows us to observe consent mechanisms as they are actually presented to local users, taking into account geographical variations, through the use of country-specific VPN connections. Second, we offer a comparative analysis that highlights qualitative differences in cookie banner design strategies and the use of dark patterns in the various jurisdictions studied. Finally, we address the consequences of these distinctions in relation to existing regulations and current restrictions on user interface-based consent mechanisms.

This article is structured as follows: Section 2 presents the theoretical and legal framework, detailing the definition and functioning of cookies, as well as the concept of consent and the legal regulatory frameworks in each country studied. In section 3, we review related work and present the state of the art. Section 4 then describes the methodology used in this research, the tools employed, and the tests carried out. Section 5 presents the results observed in this regard for each country. Section 6 is devoted to a critical analysis of the results found and the limitations of this study. Finally, it summarizes the main findings and opens up avenues for future research.

2. THEORETICAL AND LEGAL FRAMEWORK

To understand the challenges of cookie banners and consent, it is necessary to review the technical and legal basis for online data collection [9]. In this section, we will first present the role of cookies and how they function, then discuss the regulations regarding consent, and conclude with a comparison of the regulatory frameworks between the five countries selected: France, Germany, the United States, Japan and Morocco.

2.1 Definition and functioning of cookies

Cookies are small data files that are stored on the browsers of the user. The main purpose of cookies is to facilitate user navigation by storing information about preferences, for example [9]. However, over time, they have been used for other purposes. Nowadays, they are a very important tool for understanding how users behave online and for advertising [2].

Table 1 shows some types of cookies and their functions.

Technically, cookies are typically created and understood by the browser. They can be created by JavaScript or sent in the HTTP header by the server. Certain cookies are destroyed as soon as the session is terminated, while others can linger on for months or even years. Visibility and destruction of cookies depend on browser options, but most individuals have no idea of their existence or operation [10].

Table 1. Types of cookies according to their function [10]

Cookie Type	Main Function	Consent Required?	Examples
Essential Cookies	Ensure that the site functions correctly (login, shopping cart, language)	No	Language preferences
Performance Cookies	Evaluate website traffic and performance	Yes	Google Analytics
Advertising Cookies	Track users online in order to display targeted advertisements	Yes	DoubleClick
Social Media Cookies	Include third-party content	Yes	YouTube, Facebook
Third-Party Cookies	Generated and created by external domains	Yes	Advertising or analytics cookies
Persistent Cookies	Remain on the user's device, even after the browser is closed	Yes	Conversion tracking cookies
Session Cookies	Deleted once the user closes the browser	No	Temporary authentication

2.2 The concept of consent in the context of data protection

Whether through cookies or any other means, the collection of personal data from online users is very strictly regulated in terms of consent. The GDPR [4], which came into force in May 2018 in the European Union, stipulates in Article 4 that "Consent of the data subject: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" [11].

This definition implies a number of cumulative conditions [11]:

(1) Consent must be freely given: this implies that users must give their consent without any pressure. Also, the provision of services must not be conditional on the acceptance of cookies.

(2) Consent must be specific: users must know which cookies they wish to accept, for instance, advertising or analytical cookies, etc.

(3) Consent must be informed: users must be provided with clear, coherent, and accessible information, especially concerning the aim and objectives of data collection.

(4) Consent must be unambiguous: it cannot be obtained

solely through silence, continued browsing, or a pre-checked box.

In addition, if the user wants to refuse, the action must be simple and visible, as is the case for acceptance, in accordance with the recommendations of the Commission Nationale de l'Informatique et des Libertés (CNIL) [12], and other data protection authorities. Any alteration to the interface or design, such as hidden buttons or the use of less visible colors, can be interpreted as a violation, known as "dark patterns." This is a way of manipulating the user into making a decision that is contrary to their interests [13].

2.3 Legal frameworks in the five countries studied

2.3.1 France

France, as part of the European Union, applies the GDPR. It also has a very active supervisory authority, known as the CNIL [12]. In addition to the requirements of the GDPR, CNIL guidelines specifically regulate cookies. For example, refusing cookies must be as easy as accepting them, consent must be explicit, and no non-essential cookies may be present before the user has made a choice. The CNIL conducts regular checks and has already imposed significant penalties on several companies [14].

2.3.2 Germany

Germany also applies the GDPR, like France, as well as the ePrivacy Directive. What sets this country apart is its culture of protecting the privacy of online users, which is deeply rooted in its history, as well as the rigor of its authorities [11]. The Federal Commissioner for Data Protection and Freedom of Information (BfDI) and regional authorities (Länder) enforce strict oversight, and German users are generally better informed about their rights. This results in websites that are more compliant and a more faithful adherence to the principles of the GDPR [15].

2.3.3 United States

In the United States, there is no single, comprehensive law like the EU's GDPR. However, there are several federal and state laws regulate data protection and safeguard the privacy of online users. The most advanced law is the CCPA [4], which grants online users certain rights, including the right to delete or opt out of sharing their data. Since there is no mandatory cookie banner at the national level, this leads to a wide variety of practices, often unsafe, particularly outside California [16].

2.3.4 Japan

Japan has laws such as APPI [5] that mandate certain obligations for the protection of users' data online, in particular when shared with third parties. However, the law is generally viewed as more flexible than the GDPR, as its requirements have a tendency to be less specific. Cookie banners are present on some websites, but the concern remains that their content is often too vague, and it is rare to find granular consent. There is a Japanese supervisory authority, the Personal Information Protection Commission (PPC) [16], which issues recommendations but exercises less strict control than in Europe.

2.3.5 Morocco

In 2009, Morocco adopted Law 09-08 [6] to regulate the personal data protection, requiring clear user consent before collecting any personal data, including cookies. The National Commission for the Control of PPC oversees the law's application. On paper, Morocco has a framework closely mirrors the GDPR; in practice, however, enforcement is weak, and most Moroccan websites lack compliant or even visible cookie banners. Digital players largely ignore the issue, and official oversight is minimal [16].

2.4 Comparative summary

Table 2 summarizes and presents the significant differences identified between the countries studied in terms of cookie consent.

Table 2. Comparison of legal frameworks for cookie consent

Criterion	France	Germany	United States	Japan	Morocco
Main law	GDPR + ePrivacy	GDPR + ePrivacy	CCPA (California), local laws	APPI law	Law 09-08
Explicit consent required	Yes (opt-in)	Yes (opt-in)	No, generally (opt-out)	Partially (depending on the case)	Yes
Banners required	Yes	Yes	No (not at the federal level)	Varies depending on the site	Recommended
Refusal as simple as acceptance	Recommended by the CNIL	Recommended, often respected	Rarely offered	Often absent	Rarely respected
Level of real control	High (fines and audits)	Very high (prevention and rigor)	Low to medium depending on the state	Medium	Low
Privacy culture	Moderate (recent progress)	Strong (culturally ingrained)	Weak (data = economic resource)	Average (pragmatic approach)	Weak
Main law	GDPR + ePrivacy	GDPR + ePrivacy	CCPA (California), local laws	APPI law	Law 09-08
Explicit consent required	Yes (opt-in)	Yes (opt-in)	No, generally (opt-out)	Partially (depending on the case)	Yes

According to Table 2 we can see that despite having the same legal basis, France and Germany differ in the strictness of their enforcement. The U.S. still very tolerant. It has no rigorous federal structure. Japan and Morocco, have taken an intermediate and still evolving approach.

3. STATE OF THE ART

In this section, we have presented existing research on cookies and consent. Existing studies reveal that rules are not always followed and that most websites use techniques to

influence user choices.

3.1 Studies on dark patterns and consent manipulation

Since the implementation of the GDPR in 2018, many studies have shown that cookie consent banners use dark patterns (misleading interfaces) to influence users' decisions [13].

The landmark article by Célestin Matte, Nataliia Bielova, and Cristiana Santos [17], “Do Cookie Banners Respect My Choice?”, highlighted that 85% of the websites studied violate the rules of valid and informed consent by implying cookies before users have had a chance to make a choice.

Arunesh Mathur and Gunes Acar [18] conducted a large-scale analysis of more than 11,000 websites and identified 15 types of common dark patterns, such as Confirmshaming, Roach Motel, and Hidden Legalese. These strategies are designed to deceive you into consenting to cookies through cognitive biases.

Ralf Gundelach and Dominik Herrmann [19] developed “Cookiescanner,” a solution that identifies the presence of dark patterns in cookie banners: absence of a refusal button, dominant colors or sizes, questionable wording, etc.

More recently, the research conducted by McGarrigle [20], titled "Consent Banners, Dark Patterns, and GDPR Violations in Online Gambling," it was identified that a total of 86% of the websites reviewed were found to have at least one use of dark patterns present. Additionally, a number of the websites processed personal information prior to receiving user consent, thereby violating the principles of the GDPR.

Finally, Robert Viseur's [13] study, “Ethical management of consent to the processing of personal data: How can dark patterns be used to guide decision-making?” reveals that dark patterns displayed on cookie banners take advantage of users' cognitive weaknesses (such as difficulty processing complex information or susceptibility to persuasion) to influence their choices. According to the author, this is a major ethical issue, as these methods, even if sometimes legal, restrict the decision-making power of internet users.

3.2 Technical compliance and consent enforcement

Beyond the appearance of cookie banners, there are technical studies that have analyzed the behavior of websites in terms of cookie placement.

Brian Tang, Duc Bui, and Kang G. Shin in their study “Navigating Cookie Consent Violations Across the Globe” analyzed 1,793 websites across eight countries. The results indicated that the majority of these websites placed tracking cookies before obtaining the user's consent or even after the user had explicitly refused [21].

Ali Rasaii, Devashish Gosain, and Oliver Gasser, in their 2023 paper “Thou Shalt Not Reject: Analyzing Accept-Or-Pay Cookie Banners on the Web,” analyzed “cookiewalls” and found that they are binary choice devices: either you pay or you accept cookies—a very convenient way to circumvent the spirit of the GDPR. Websites using this type of model deposit up to 6.4 times more third-party cookies [22].

Tests on automatic extensions, such as Consent-O-Matic (Midas Nouwens and Ilaria Liccardi [23]), have shown that some sites deposit tracking cookies even when the user explicitly refuses, revealing a technical violation of the choice expressed.

According to a 2024 study by Advance-Metrics, which looked at the behavior of 1.2 million users, nearly 70% of visitors see or close cookie banners, raising questions about the implicit interpretation of consent [24].

At the institutional level, the French Data Protection Authority and the German Federal Commissioner for Data Protection and Freedom of Information sanctioned websites in 2023–2024 that used banners that made refusal impossible or difficult [25].

3.3 Limitations of previous research

Although this research has been increasingly successful, it nevertheless has several major shortcomings. Much of it focuses on Western European and North American countries. Considered law 09-08 for Morocco and the APPI for Japan, shows how Morocco and Japan still get overlooked even with their different economic and financial architectures.

The vast majority of existing studies are declarative or legal in nature. Very few attempt to provide a technical analysis of the cookies actually stored and, in the context of consent, to use scripts that would automate the user journey.

Many studies do not take into account the actual impact of dark patterns on Moroccan or Asian users, whose browsing habits, language, and level of acceptability can be very different.

Finally, there are still few cross-sectional studies comparing several countries with different legal contexts. This reinforces the value of your work, which aims to analyze five countries—France, Germany, the United States, Japan, and Morocco—using a common methodology and objective technical criteria.

4. METHODOLOGY

This study uses a comparative approach to determine if websites are truly willing to follow user preferences regarding the acceptance or rejection of cookies. Our approach combines technical analyses with a detailed analysis of local regulatory requirements in the five selected countries, which have different approaches to user privacy on the Internet.

4.1 Website selection

The Tranco list was used to select most of the websites analyzed in this study, which incorporates several popularity rankings to minimize the bias associated with a single source. Websites from each country studied, namely France, Germany, the United States, Japan, and Morocco, were ranked according to their country code top-level domain (e.g., .fr, .de, .jp, .ma).

Subsequently, websites were automatically classified into five functional categories—media, e-commerce, health, education, and public administration—using heuristic rules based on domain names. Sites in each category were tested according to their Tranco ranking until a fixed number of accessible sites was reached. Sites that were not accessible or that caused technical errors were removed from the final corpus.

In the case of Morocco, the number of accessible websites in the Tranco list is insufficient for certain categories. In order to ensure comparable coverage across categories, we have added a limited number of additional sites. The sites selected are widely used public and private services that have a national domain (.ma) and strictly correspond to the categories studied.

All these sites underwent the same automated testing protocol as those from the Tranco list.

4.2 Experimental environment and geolocation

The Chromium browser was employed during the testing process, which was automate with the use of the Playwright library to provide a real-world browsing experience. The testing occurred in a protected environment, where each test was conducted on a new session of the Chromium browser that had not been cached or had any previous cookies.

To take into account the different ways that consent and tracking are done throughout countries, all measurements were done through country-specific VPN's. Therefore, for each series of tests, a Proton VPN server that was physically located in the country being tested was activated. This approach allows us to observe consent interfaces and technical behaviors as they are actually presented to local users.

Some sites are known to detect or block VPNs. However, this effect is considered similar across the countries studied and therefore does not introduce significant bias into the comparison.

4.3 Automated test procedure

To enhance the understanding of the experimental protocol, Figure 1 demonstrates the various phases of the automated procedure for assessing consent mechanisms.

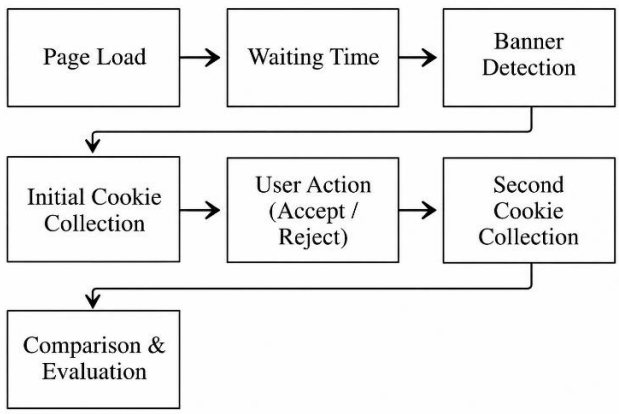

Figure 1. Diagram of the automated process for evaluating cookie consent mechanisms

For each website, the homepage was accessed via HTTP or HTTPS protocols, with requests repeated to minimize the risk of errors caused by loading issues. We then waited a few seconds to ensure that all banners were properly displayed and scripts were activated.

We then performed an initial collection of trackers. A consent banner was detected when text regarding the use of cookies was associated with visible action buttons (e.g., «Accept», «Reject», or «Settings») on the page.

The user simulated an interaction as much as possible by clicking the link corresponding to the option to reject. A new collection of trackers was then implemented, with the aim of identifying persistent cookies after refusal.

In this way, it will be easy to compare the traces collected before the interaction with those that exist afterward, thereby determining to what extent the user's choice is implemented from a technical standpoint.

4.4 Detection of third-party trackers and deceptive design patterns

Third-party cookies were identified based on their domains by cross-referencing domain discrepancies (where the cookie's domain does not match the website's main domain) with a list of the most commonly used tracking services (Google Analytics, Facebook, Criteo, Taboola, Hotjar, etc.).

In addition, several dark patterns are identified by heuristic rules. For example, on some sites, the "Accept" button is highlighted in terms of color or size, while the "Reject" option appears less accessible or requires several additional clicks to reach. Other interfaces rely on visible checkboxes or ambiguous wording that can be misleading. More subtly, the outright absence of an explicits opt-out option or the use of implied consent is also encountered.

These examples illustrate the main dark patterns identified in this study. This approach is not intended to be exhaustive, but rather to highlight fairly obvious mechanisms that may influence the user's choice.

4.5 Construction and calculation of the Cookie Compliance Score

By summarizing these observations collaboratively, a CCS was calculated for each website. This binary score, ranging from 0 to 5, is derived from five binary criteria designed to cover the most critical aspects of the technical robustness of cookie consent mechanisms.

The selection of these criteria is based on both regulatory principles and existing research on consent mechanisms. More specifically, the GDPR requires that consent be freely given, specific, informed, and unambiguous. The selected criteria were therefore defined to verify whether websites technically respect the user's choice. In particular, they include the absence of third-party cookies prior to obtaining consent, the presence of a clear and accessible opt-out options, the absence of implied consent or pre-checked options, as well as the presence of a visible opt-in option.

A website that meets each criterion receives a score of 1; otherwise, it receives a score of 0. Another decision made was to avoid gray areas as much as possible in order to ensure a simple and reproducible evaluation. These criteria are combined to provide a summary measure (the CCS) for each site, making it easier to compare the differents sites examined.

The purpose of the CCS is not to assess whether websites are legally compliant or not, but rather to quantify the gap between the consent expressed by the user and the tracking practices deployed. Thus, a low score indicates that the user's choice and the site's technical behavior are more likely to be inconsistent, which could be associated with a higher risk to privacy and personal data protection.

4.6 Collection, traceability, and ethical considerations

All results are recorded in a CSV/Excel file, accompanied by a detailed log summarizing all browsing activity, cookies found, actions performed, and any errors that occurred. This ensures that experiments can be reproduced and that results data can be consulted retrospectively.

The research focused exclusively on public websites, with no interaction between websites and user accounts and no personal data. No individual information was retrieved during the test. The detailed automated data collection protocol is provided in Appendix.

5. RESULTS

5.1 Global comparative analysis between countries

The average CCS scores for the five nations studied - France, Germany, Japan, USA, and Morocco are shown in Figure 2. France has the highest average rating of approximate (≈4.3/5), while Germany has a slightly lower average of approximately (≈3.7/5). Japan has a middle rating of approximately (≈2.9/5) and the USA and Morocco have lower ratings, at approximate ratings of (≈2.2/5) and (≈1.3/5) respectively.

The results above indicate that there is a strong correlation between the level of strength in regulatory framework, and the corresponding level of compliance observed. Countries that operate under GDPR, like France and Germany, typically demonstrate higher rates of compliance, likely due to their enforcement processes being more rigorous and through having an active regulatory authority. However, the correlation should be viewed cautiously, due the possibility of other contributing factors that may also affect compliance, including but not limited to financial incentives, industry standards and the technological sophistication of individual organizations.

Morocco, on the other hand, has a notably lower CCS score and the reasons for this score can be attributed to several elements, including weaker levels of enforcement, lower levels of institutional pressure or weaker standards with which to implement consent protocols. Overall, in such an environment, it's likely to find that compliance practices are heterogeneous in nature and are less frequently integrated into website designs in a systematic manner.

5.2 Analysis by website category

Figure 3 shows the average CCS Score of countries across all categories (education, government, health, e-commerce and media), with education having the highest compliance score (≈3.3) and government second highest (≈3.1) while healthcare (≈2.7), e-commerce (≈2.7) and media (≈2.6) tend to show lower compliance scores than education and government.

These results indicate a tendency for government and semi-government entities to establish stronger consent systems because they experience greater institutional pressure, more extensive regulatory supervision, and greater understanding of their legal responsibilities regarding protection of personal information. Compliance is often based in the formal governance framework in these contexts, leading to a greater likelihood of consistent implementation.

In comparison e-commerce and media show a much more variable approach to compliance. A major factor in this may be the economic advantages associated with data collection and advertisement via tracking, which are critical to their business model. Thus, they are often forced to weigh the benefits of compliance with the costs of maximizing revenue.

The differences in these two sectors should not be viewed exclusively from an economic perspective. Differences in technology infrastructure, organizational experience and the complexity of integrating consent systems may also account for some of the differences between sectors.

5.3 Country and category interaction

The heatmap in Figure 4 shows the interactions between countries and categories.

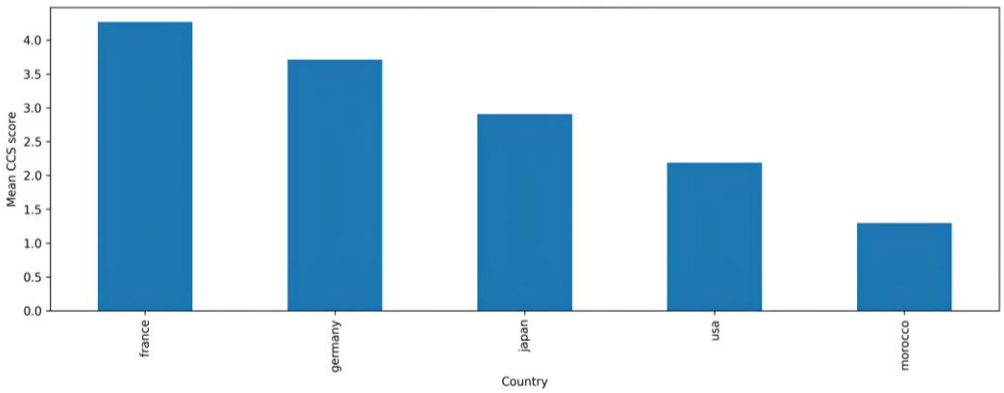

Figure 2. Mean Cookie Compliance Score (CCS) by country

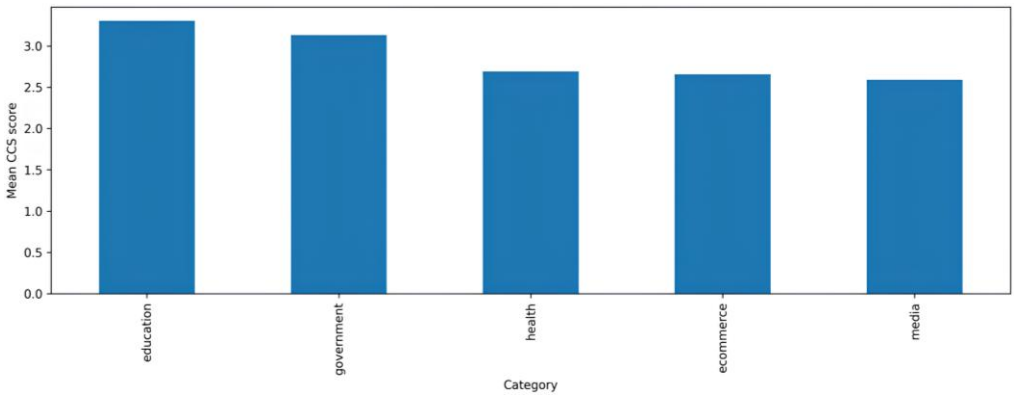

Figure 3. Mean Cookie Compliance Score (CCS) by category

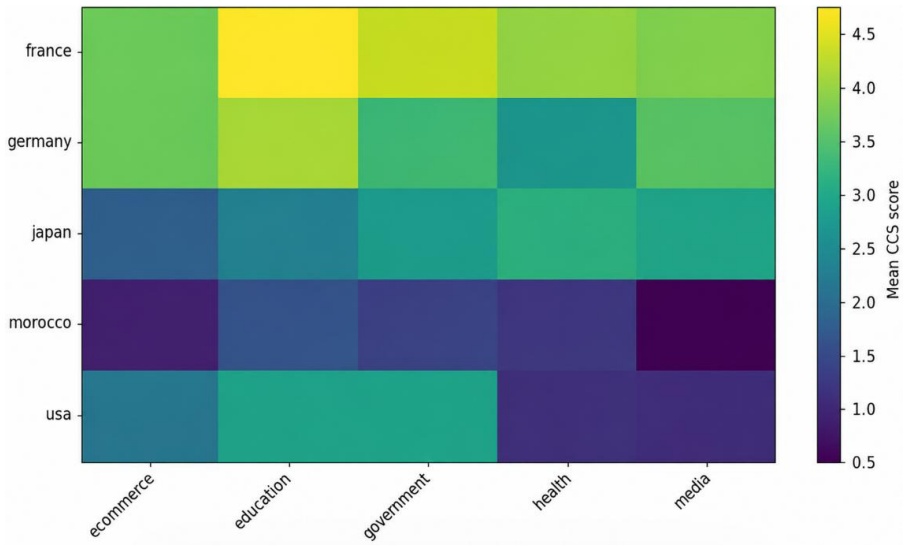

Figure 4. Heatmap of the mean Cookie Compliance Score (CCS) by country and category

5.3.1 France

France shows a notable and consistent level of compliance across all categories, with particularly strong results in the areas of education and government affairs (around 4.7–4.8). The areas of e-commerce and healthcare also show high scores (> 4).

The main reason for these strong results is that the GDPR is enforced very strictly in France. The CNIL, in particular, ensures that websites comply with personal data protection rules and does not hesitate to impose fines when it detects violations. As a result, companies have every interest in implementing robust consent-gathering strategies and ensuring they are effective. Furthermore, the public and the education sector are often particularly transparent, which contributes to their high levels of trust.

5.3.2 Germany

Germany has a profile similar to that of France, although the results are slightly lower. The level of compliance appears to be fairly consistent across different sectors.

This can be interpreted as the result of a robust legal framework based on the GDPR. The differences observed compared to France can be explained by variations in the rigor of oversight or in corporate practices. The similarity in results indicates that compliance is influenced more by national regulations than by sector-specific factors.

5.3.3 Japan

Japan's compliance level is medium in most areas, with the country's health and media sectors showing slightly better performance than e-commerce.

The reason for this pattern might be the different focuses of regulation and different market behaviors. Japan's better relative results in the health sector could indicate that people here are more aware of their personal data in this industry, while at the same time, e-commerce's low level of compliance might be due to companies' increased use of online user tracking for commercial purposes. In fact, this means that the profit motives of certain industries are resulting in varying levels of compliance.

5.3.4 United States

The United States has a mixture of positive and negative results. In fact, the government and e-commerce categories get moderate scores whereas the media and health care categories score much lower.

One of the reasons for such difference could be the complex structure of the U.S. regulatory framework for privacy protection where laws differ from state to state and also from one industry to another. Besides that, some industries, like the media, depend a lot on the advertising business models which sometimes encourage even the loosest surveillance practices and also result in non-compliance to laws.

5.3.5 Morocco

Morocco generally scores low across all categories, with particularly poor performance in the areas of media and e-commerce. It appears that compliance is, on the whole, limited and poorly organized.

This finding may be due to less rigorous enforcement of existing rules or less institutional pressure. The differences observed across sectors indicate that compliance methods have not yet been standardized and rely more on each organization's specific approaches than on a set of strict rules.

These results suggest that the national regulatory framework is more decisive than sectoral differences when it comes to structuring compliance levels. Countries with a stricter enforcement of regulations have higher and more homogeneous scores whereas less stringent regulatory environments give rise to lower and more variable compliance levels. However, sector-specific economic incentives, especially those based on advertising, also explain differences to some extent.

5.4 Distribution of Cookie Compliance Score scores

The distribution of CCS values shown in Figure 5 gives us a clearer picture of compliance variability among different countries. France and Germany have a significant portion of their websites receiving the maximum possible CCS value (CCS = 5). This demonstrates that there is a high level of adoption of adequately structured consent mechanisms which comply with all of the various technical and interface requirements. Additionally, the fact that so many websites received CCS values of 5 indicates that they are most likely subject to significant regulatory influence and that website compliance levels are relatively consistent amongst themselves.

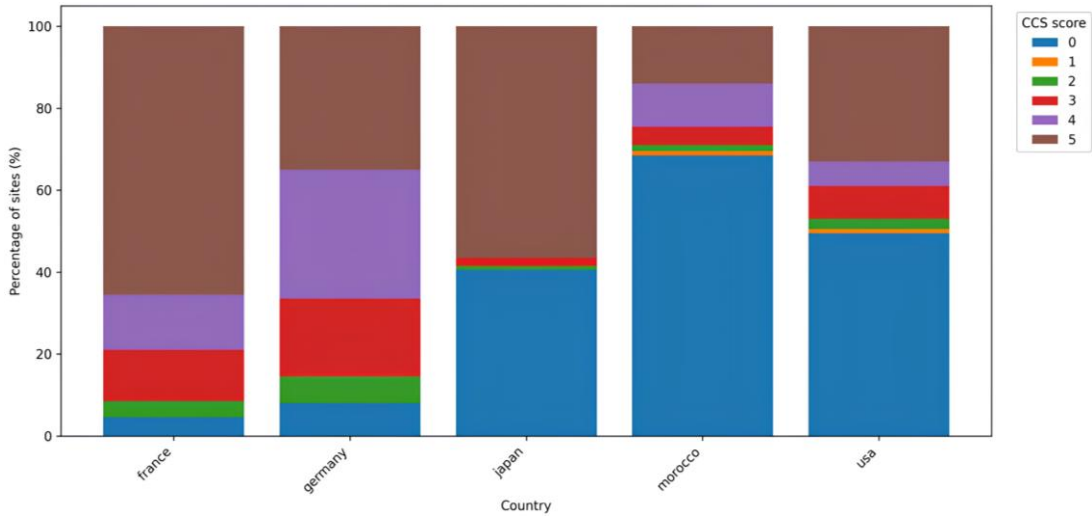

Figure 5. Distribution of Cookie Compliance Score (CCS) by country

On the other hand, there is a considerable skew in the distribution of CCS values for Morocco with most scores being either low (0 or 1); this means that there has been little or no adoption of structured consent mechanisms. This unequal distribution pattern could be explained by a lower level of enforcement and institutional pressure and a lack of a standard process for implementing consents. The absence of higher scores indicates that there are still very few websites complying with advanced compliance best practices in this area.

The data for Japan shows a more evenly distributed set of scores, with the majority of scores along the middle of the distribution. One interpretation of this finding is that some of the consent mechanisms have been partially implemented by organizations, so that some of the requirements have been met while other ones have not been implemented consistently. The fact that Japan is likely somewhere in transition along the continuum of adopting privacy practices and is being influenced by both its regulatory frameworks and the constraints of various sectors contributes to this distributional pattern.

The data for the US shows a much higher level of variability across all 3 cases than does Japan. In fact, there are so many instances of low ratings for organizations that the overall mean rating for US organizations is quite low. This variability may indicate that organizations' compliance practices differ substantially from organization to organization due to the very fragmented nature of the regulatory environment in the US. Therefore, in the absence of a uniformly applied regulatory framework for compliance, the implementation of privacy practices has been driven much more by the strategies of individual organizations (the internal pressures) rather than through a common set of external pressures.

5.5 Cookie banner detection rate

As the data in Figure 6 shows, the detection rate of cookie banners varies quite a bit across the five countries analyzed. In France, 62% of the websites analyzed contained a consent banner, while 60% of the websites surveyed in Germany had one as well, but websites in the US had a significantly lower detection rate (23%) and Morocco (19%) had an even lower detection rate. The least number of websites detected with a consent banner were in Japan (5%).

The data indicate that cookie banner visibility is very much dependent on the regulatory framework. It appears that in the EU, where user consent is a requirement under GDPR, cookie banners have become institutionalized. A high detection rate is indicative of the fact that most websites at a minimum are complying with the requirement of a cookie banner.

In contrast, the considerably lower detection rates reported from countries outside Europe may indicate there are generally no or poorly-enforced laws about them; however, the differences should not just be seen as having a regulatory impact. Various other factors can play a role including, local differences in how it’s done, different user expectations, and the use of alternative methods that don’t rely on an explicit consent interface for tracking.

The presence of a banner is not, however necessarily indicative of compliance as noted above. There are instances when it might merely represent a formal obligation to provide a banner without the user really giving their consent based on proper usage of said consent. This indicates the necessity for building on banner detection with more detailed measures (e.g., CCS) to determine the real validity of the mechanism used to provide consent.

5.6 Prevalence of dark patterns

Figure 7 illustrates the proportion of websites displaying at least one of the dark patterns detected. The results show that the distribution of these manipulative mechanisms varies greatly between countries, with 45% of German websites and 36% of French websites displaying at least one manipulative mechanism, while this number does not exceed 17% for American websites, 15% for Moroccan websites, and only 3% for Japanese websites.

One particularly interesting result stands out: the countries with the highest levels of formal compliance are also those with the highest proportion of dark patterns.

This suggests that strict regulations encourage the implementation of consent banner, but that some actors also use influencing strategies, such as visual asymmetry between the «accept» and «decline» buttons, the non-visibility of the decline option, implicit consent, etc., to influence the user's choice.

This observation highlights the phenomenon of « strategic compliance », which consists of formally complying with legal requirements while partially circumventing them through design mechanisms that may alter freedom of consent.

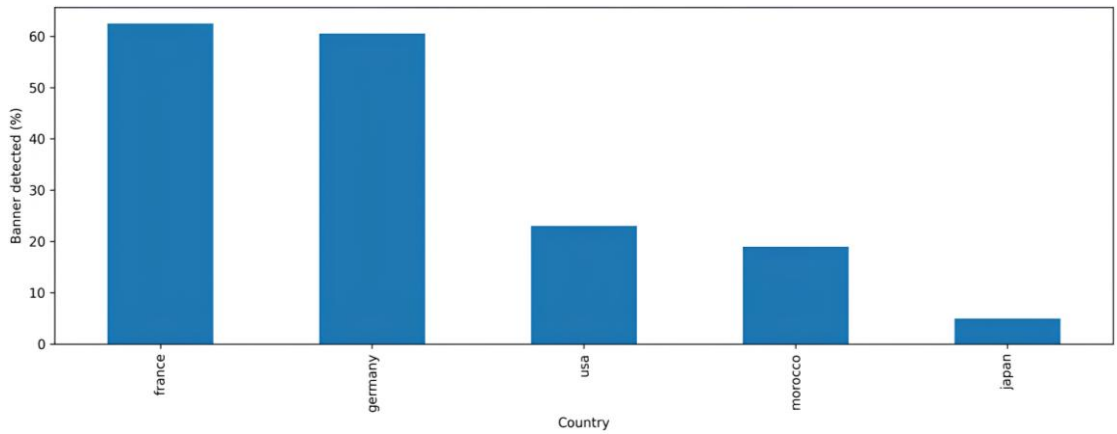

Figure 6. Cookie banner detection rate by country

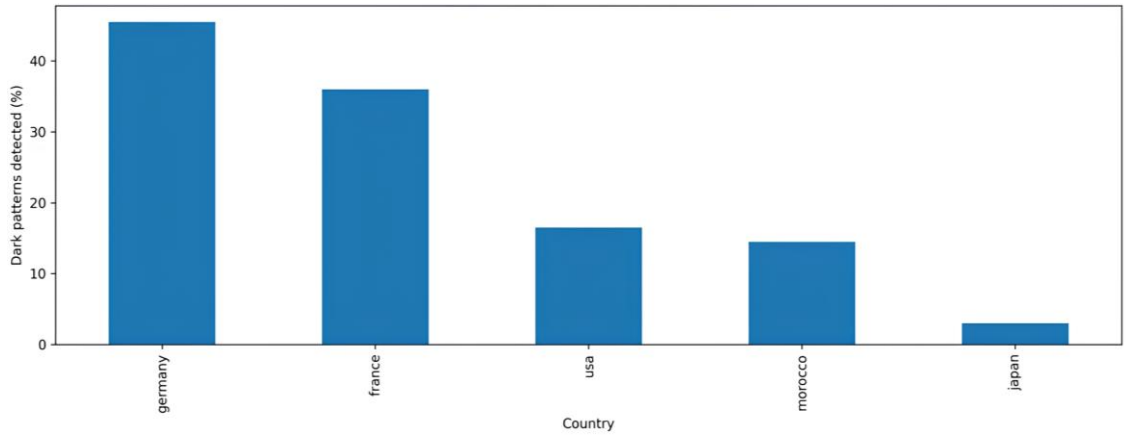

Figure 7. Dark patterns rate by country

5.7 Summary of results

The results show a significant difference between countries in how they follow cookie rules. European countries have the highest compliance scores, both overall and in terms of the presence of banners.

Educational and government domains are characterized by a high level of compliance compared to commercial domains. Finally, the existence of a high level of compliance and a strong presence of dark patterns in certain countries raises doubts about the real effectiveness of the regulatory mechanisms in place.

6. DISCUSSION

6.1 Effect of the regulatory framework and institutional pressure

These highlight the considerable differences between the countries analyzed, suggesting a strong correlation between the regulations to which they are subject and the level of compliance observed. France and Germany obtaining high scores has bolstered the idea that there exists a positive correlation between a stringent regulatory environment, such as the GDPR, and the procedural implementation of explicit consent mechanisms.

One could see this as coercive isomorphism being manifested through institutional theory. Organization operating in highly regulated environments tend to adopt compliant practices in order to avoid legal or reputational sanctions. The significant differences observed between European Union countries and non-EU countries can be taken as an indication of the structural effect of regulatory constraints in the development of these methods of formalizing consent management systems.

However, caution should be exercised in interpreting the causal conclusions drawn. This article highlights strong correlation between the regulatory context and observed compliance, but other variables, such as digital maturity, societal pressure, and organizational culture, may also explain some of the differences observed.

6.2 Sectoral differences and economic incentives

Analysis by category reveals that educational and government websites generally show higher compliance with laws and regulations compared to economic sectors like media and e-commerce. One reason for this could be different incentive structure. Public institutions, usually, not only have stricter transparency requirements, but they are also subject to stronger institutional controls which may lead to the implementation of compliant mechanisms.

However, sectors that rely primarily on behavioral advertising and datas revenue may face a strategic trade-off between formal compliance and more effective value creation. The collection of behavioral data is the key lever for value creation in the media and e-commerce sectors. Consequently, the design of consent mechanisms is influenced by the desire for maximum acceptability, rather than the administration of a

perfectly neutral choice.

These findings are consistent with research on data governance and the tensions between legal compliance and digital business models.

6.3 Formal compliance and dark patterns: The paradox of regulation

One of the most striking aspects of this study concerns the coexistence, in certain countries, of a high level of formal compliance and a high incidence of dark patterns. European countries, which have the highest average scores, also have the highest rates of potentially manipulative design mechanisms.

This phenomenon can be interpreted as one type of "strategic compliance" or "regulatory gaming." For example, if the regulation requires the explicit inclusion of both accept and decline buttons, the designer can be getting the formal part of the rule right though at the same time designing the choice architecture in a way which will influence the user's choice. This first is related to the studies done on nudge theory and choice architecture which highlight that the way options are presented can be a major factor in the decision-making of people even those who explicitly consent.

It could therefore be said that regulation has a paradoxical effect: the higher the level of procedural compliance, the more sophisticated the influencing strategies. This confirms that, at all times, there is a fundamental distinction between formal compliance (compliance with the written requirements of the rules) and substantive compliance (compliance with the principles of the GDPR and the principles of decision-making autonomy).

6.4 Implications for regulation and interface design

This study shows that privacy laws should require not just consent banners but also stipulate exact specifications on user interface design. Just making choices visible is insufficient, as this may lead to only shallow or strategic compliance behaviors ("compliance" here being the minimum threshold of behavior required for sites to meet their requirements whilst still manipulating users' decisions).

The research results particularly highlight the necessity of enforcing principles such as visual neutrality, equal visibility of the accept and refuse options, and banning manipulating interfaces. From this point of view, the elaboration of automated auditing instruments that facilitate the assessment of interface compliance has a huge potential to significantly improve the regulatory control effectiveness.

Besides the regulatory and ergonomic issues, these findings also reveal serious safety and data protection challenges. If consent mechanisms are poorly designed, especially when third-party cookies are involved, users may be more exposed to cross-site tracking, profiling of their habits, and leaking of data to external players. And when, on the technical side, the choices expressed by users are not effectively implemented, a gap arises between what they think they have decided and what the system does. This may then be seen not only as a compliance issue but also as a security vulnerability.

Opening up the discussion, this paper is one of the wider discourses that discuss digital regulation efficiency. On one hand, legal frameworks can really help enforcement; however, they are not guaranteed to be successful protection of user freedom. For future regulations, this is a very good point for consideration of behavioral, ergonomic, and technical issues, including safety ones.

6.5 Interpretive synthesis

Overall, the findings suggest that user-consent levels for cookie-consent tools that ask users for their permission differ significantly not only between various legal systems but also between different industries. We can observe formal compliance practices more frequently in the well-supervised scenarios. Yet, it is such cases only where the greatest number of design-based ways of obtaining users' consent can be found. On the whole, people tend to be more compliant with rules in public places than in private shops, which may be a reflection of different levels of institutional pressure and incentives for organizations.

Besides highlighting the difficulty of measuring compliance in the digital world, these results emphasize that the presence of a rule alone is not sufficient for its success. Besides merely existing, a regulation's effectiveness hinges on the capacity to give clear guidance to the interface methods and the corresponding technical solutions.

Therefore, the CCS can be considered a measure of how well the user's consent expression is aligned with the system's permission. A high score reflects well-designed consent-gathering methods. On the other hand, a low score points to a strong discrepancy between users' understanding of their choices and the reality of the tracking behavior.

But these differences, however, are not only rule-breaking issues; in fact, they can become threats to data protection as well. It is a fact that non-compliant consent collection can be a cause of cross-site tracking, marketing-oriented tracking, and data exposure to resource pools. Therefore, CCS is not simply narrative description but also a way to discover privacy and security challenges brought about by particular conducts.

Therefore, the CCS may be considered a reflection of the degree of alignment between what users have declared as their consent and what the system actually allows them. A high score indicates that the consent collection methods employed are appropriate. Conversely, a low score implies that there is a significant divergence between user-perceived choices and the actual tracking methods used. But beyond just rule compliance problems, these misunderstandings can even endanger data protection. Indeed, not adhering to consent collection guidelines can result in cross-site tracking, marketing tracking, and even data leaks to resource pools. Hence, the CCS is not only a way of describing matters but it is also a means to identify privacy and security issues linked with human behaviors.

6.6 Study limitations

Although this study is wide-ranging and comparative in nature, it nonetheless has certain limitation that must be highlighted in order to interpret the results with caution.

First, this analysis is based on automated data collection carried out at a specific point in time. However, cookie consent collection mechanisms are constantly changing and can evolve very quickly due to technical update, regulatory changes, or court decisions. This is therefore a snapshot of current practices and in no way a permanent state of affairs. A longitudinal study would be needed to analyze the evolution of compliance strategies and the effect of regulations.

Subsequently, the choice of sites is based primarily on the Tranco site ranking, supplemented to achieve a fixed number

of samples per category and per country. While this approach has the merit of covering most of the most visited sites, it is not without bias. Indeed, the habits of high-traffic sites, which can rely on often large technical teams, may differ from those of small structures or sites with a local audience. Care must therefore be taken not to extrapolate the findings beyond the sites selected in each country.

The sample utilized for some countries has another constraint; i.e. the sample chosen for Morocco is limited by the daily selection method used to identify the websites in the sample. Because the chosen websites do not represent the larger national web ecosystem, the results from the Moroccan websites should be used with caution and compared directly with results from other countries.

Secondly, the CCS and dark pattern detection are based on criteria defined in the literature and recommendations issued by regulatory authorities. While they enable standardized and reproducible compliance measurement, they necessarily simplify the complexity of digital interfaces. There are some subtle things, such as a slightly different visual hierarchy, typography detail, lexical choices, and animation dynamics, that content detection software may simply not catch. Conversely, features that are identified as potentially indicative of manipulation may actually be the result of technical limitations rather than intentional strategic decisions.

Furthermore, the study focuses mainly on what is visible in terms of user interface compliance. It does not assess backend compliance, particularly in the case of pre-buffering, to ensure that non-essential cookies are effectively blocked after consent has been refused. The network level (firewall, proxy, clicking on the cross, etc.) would need to be checked to verify that clicking on "refuse" has been taken into account.

Another limitation is that it does not take into account aspects such as digital culture, users' level of awareness of data protection, or the intensity of the actual enforcement of sanctions by country. These differences can be explained by institutional and sociocultural factors, which may be a avenue for future research.

Finally, although significant differences were observed between countries and sectors, this study is essentially limited to a descriptive comparative approach. To substantiate such a causal relationship between the regulatory framework and the level of compliance, it would be necessary to go further in the statistical analyses and use more explanatory variables.

Beyond these weaknesses, this study provides a consistent comparative mapping of current methods for obtaining consent for cookies and represents a rich source of information for future research, whether it concerns the evaluation or monitoring of the implementation or effectiveness of data protection policies.

7. CONCLUSION

The aim of this study was, on the one hand, to compare cookie consent management practices across five countries with different regulatory frameworks and, on the other hand, to assess the quality of various forms of consent based on a sample of 1,000 websites from five different industries. The CCS is a composite indicator used to measure the quality of consent mechanisms, as well as the extent to which they may involve manipulative design patterns.

The results show that there are big differences in scores between countries. European Union countries, which follow the GDPR, have much higher levels of compliance than countries outside the Union. This confirms the important role a regulatory framework can play and how effective oversight mechanisms are in shaping digital practices. These results also indicate that the levels of formal compliance do not necessarily ensure that the users' autonomy to make informed choices is respected, especially when design mechanisms are likely to influence their choices.

The sectoral analysis reveals disparities in compliance levels among public, educational, and commercial entities: the former demonstrates better compliance practices than the latter, which could take the form of an "economic incentive," safeguarded by data processing in accordance with the GDPR.

This study also confirms the prevailing concern in the digital space regarding ensuring the security of information systems (or the fear of non-compliance with consent), rather than ensuring that consent is properly respected—which involves, in particular, rejecting persistent trackers, third-party cookies used for tracking across different sites, "behavioral profiling," or data leaks.

What makes this mechanism a legal requirement is that it also plays a great role in ensuring the security of web systems.

The results of this research show that changes should be made to the law that clearly set the standards for interface design, make technical systems more visible, and regulate the use of trickery. Meanwhile, creating automated auditing tools might be a great way to improve supervision.

Finally, this research opens up several avenues for further study, both regarding the investment required for longitudinal studies that would allow us to observe changes in practices over time and regarding the qualitative approaches to adopt to better understand the interactions between users and consent interfaces. This work will enrich academic debates while helping to identify avenues for better guiding public data protection policies in the era of platform digitization.

ACKNOWLEDGMENTS

The authors would like to express their gratitude to the members of the Intelligent Processing and Security of Systems (IPSS) laboratory at Mohammed V University in Rabat for their supportive environment and insightful discussions during the preparation of this work.

REFERENCES

[1] El-Yahyaoui, A., Omary, F. (2021). An improved framework for biometric Database's privacy. International Journal of Communication Networks and Information Security, 13(3): 499-510. https://doi.org/10.17762/ijcnis.v13i3.5143

[2] Demir, N., Theis, D., Urban, T., Pohlmann, N. (2022). Towards understanding first-party cookie tracking in the field. Arxiv Preprint Arxiv:2202.01498. https://doi.org/10.48550/arXiv.2202.01498

[3] Jo, A.M. (2024). The unexpected effects of the GDPR on competition in the online advertising market. https://hal.science/hal-04315721v1.

[4] Hosseini, H., Utz, C., Degeling, M., Hupperich, T. (2024). A bilingual longitudinal analysis of privacy policies measuring the impacts of the GDPR and the CCPA/CPRA. Proceedings on Privacy Enhancing

Technologies, 2: 434-463. https://doi.org/10.60882/cispa.25771329
[5] Kirchhoff, U., Schiebe, T. (2017). The reform of the Japanese act on protection of personal information. From the practitioner's perspective. Zeitschrift für Japanisches Recht, 22(44): 199-212.
[6] Tassinari, F. (2021). The externalization of Europe's data protection law in Morocco: An imperative means for the management of migration flows. EuroMediterranean Journal of International Law and International Relations Issue, 9: 1504. https://doi.org/10.25267/Paix_secur_int.2021.i9.1504
[7] El-Yahyaoui, A., Omary, F. (2022). A like ELGAMAL cryptosystem but resistant to post-quantum attacks. International Journal of Communication Networks and Information Security, 14(1): 132-136.
[8] Krisam, C., Dietmann, H., Volkamer, M., Kulyk, O. (2021). Dark patterns in the wild: Review of cookie disclaimer designs on top 500 German websites. In Proceedings of the 2021 European Symposium on Usable Security, New York, United States, pp. 1-8. https://doi.org/10.1145/3481357.3481516
[9] Sipior, J.C., Ward, B.T., Mendoza, R.A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. Journal of Internet Commerce, 10(1): 1-16. https://doi.org/10.1080/15332861.2011.558454
[10] Wagner, P. (2020). Cookies: Privacy risks, attacks, and recommendations. Attacks, and Recommendations. https://doi.org/10.2139/ssrn.3761967
[11] Bakare, S.S., Adeniyi, A.O., Akpuokwe, C.U., Eneh, N.E. (2024). Data privacy laws and compliance: A comparative review of the EU GDPR and USA regulations. Computer Science & IT Research Journal, 5(3): 528-543. https://doi.org/10.51594/csitrj.v5i3.859
[12] Bernelin, M., Boutet, A. (2025). PIA: Enseigner la protection des données personnelles dans l'interdisciplinarité. In RESSI: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information, Quimper, France, pp.1-5. https://www.pepr-cybersecurite.fr.
[13] Viseur, R. (2025). Éthique de la gestion du consentement au traitement des données à caractère personnel: Comment les dark patterns permettent-ils d'orienter la prise de décision des internautes?. Revue Ouverte d'Ingénierie des Systèmes d'Information, 5(1): 95-120. https://doi.org/10.21494/iste.op.2025.1301
[14] Oxman, B.H., Shelton, D. (2002). International Decisions. AM. J. INT'L L., 96: 198-205. https://doi.org/10.1017/ajil.2020.5
[15] Ramiro, A. (2025). Democratic oversight of government hacking by intelligence agencies: A critical analysis of Brazil and Germany. Weizenbaum Journal of the Digital Society, 5(2): 3. https://doi.org/10.34669/wi.wjds/5.2.3
[16] Lim, S., Oh, J. (2025). Navigating privacy: A global comparative analysis of data protection laws. IET Information Security, 2025(1): 5536763. https://doi.org/10.1049/ise2/5536763
[17] Matte, C., Bielova, N., Santos, C. (2020). Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework. In 2020 IEEE Symposium on Security and Privacy (SP), Francisco, CA, USA, pp. 791-809. https://doi.org/10.1109/SP40000.2020.00076
[18] Mathur, A., Acar, G., Friedman, M.J., Lucherini, E., Mayer, J., Chetty, M., Narayanan, A. (2019). Dark patterns at scale: Findings from a crawl of 11K shopping websites. Proceedings of the ACM on human-computer interaction, 3(CSCW): 1-32. https://doi.org/10.1145/3359183
[19] Gundelach, R., Herrmann, D. (2023). Cookiescanner: An automated tool for detecting and evaluating GDPR consent notices on websites. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, pp. 1-8. https://doi.org/10.1145/3600160.3605000
[20] McGarrigle, J., Torrance, J., Quigley, M., Dymond, S. (2026). Consent banners, dark patterns, and GDPR infringements in online gambling: Evidence from a systematic audit and online experiment. SSRN. https://ssrn.com/abstract=6477560.
[21] Tang, B., Bui, D., Shin, K.G. (2025). Navigating cookie consent violations across the globe. In Proceedings of the 34th USENIX Conference on Security Symposium, Seattle, WA, USA, pp. 5817-5836. http://arxiv.org/abs/2506.08996.
[22] Rasaii, A., Gosain, D., Gasser, O. (2023). Thou shalt not reject: Analyzing accept-or-pay cookie banners on the web. In Proceedings of the 2023 ACM on Internet Measurement Conference, Montreal, QC, Canada, pp. 154-161. https://doi.org/10.1145/3618257.3624846
[23] Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, pp. 1-13. https://doi.org/10.1145/3313831.3376321
[24] Gosteli, R. (2025). Cookie Behaviour Study – 5 years after GDPR | Advance Metrics. https://www.advance-metrics.com/en/blog/cookie-behaviour-study/.
[25] CNIL. (2025). Bannières cookies trompeuses: La CNIL met en demeure des éditeurs de sites web. https://www.cnil.fr/fr/bannieres-cookies-trompeuses-la-cnil-met-en-demeure-des-editeurs-de-sites-web.

NOMENCLATURE

APPI	Act on the Protection of Personal Information
BfDI	Federal Commissioner for Data Protection and Freedom of Information
CCPA	California Consumer Privacy Act
CCS	Cookie Compliance Score
CNIL	Commission Nationale de l'Informatique et des Libertés
GDPR	General Data Protection Regulation Cookie
PPC	Personal Information Protection Commission

APPENDIX

Appendix A. Automated data collection protocol

The empirical analysis relied on an automated data collection protocol that was implemented with the Playwright framework. A browser controlled by the script was automatically opening each site in the dataset one by one to

check for the presence and characteristics of cookie consent mechanisms.

The code logged several things such as the presence of a cookie consent banner, the presence of options to accept/reject cookies, the presence of pre-checked options, and the activation of third-party cookies before user consent. Besides that, possible dark patterns in the design of consent interfaces were identified and documented.

All gathered measures contributed to the calculation of the Cookie Compliance Score (CCS), which is a composite indicator created to estimate the extent to which websites abide by the legal requirements of obtaining user consent.