sustainability

MDPI

Article

Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations

Ognjen Pantelic, Kristina Jovic * and Stefan Krstovic

Department of Information Systems, Faculty of Organizational Sciences, University of Belgrade, 11000 Belgrade, Serbia; ognjen.pantelic@fon.bg.ac.rs (O.P.); stefan.krstovic@fon.bg.ac.rs (S.K.)
* Correspondence: kristinajovic1996@gmail.com

Abstract: This paper will mostly focus on the analysis of the implementation of cookies and their impact on the data collected from users. The first part of the paper will describe the basic characteristics and concepts of cookies. Their functionalities, categories and possibilities for creation will be presented, as well as the role of the privacy management software and its importance in cookie processing. The last part of the paper will deal with the impact of cookies on user privacy, with reference to two important regulations related to the protection of user privacy (GDPR and CCPA). The processing refers to the technological goals and challenges that arise from the introduction of data protection principles as well as the possibility of overcoming the gap between GDPR and CCPA requirements and technical capabilities. Finally, a description of the general concept of cookies is provided, with the advantages and disadvantages of their introduction. Comparing the approaches of working with cookies contributes users' insight into their specifications in order to correctly draw conclusions about the implementation of cookies. The authors give proposals and critical opinions on safety and potential directions for future development.

Keywords: software; cookies; data; privacy; security; GDPR; CCPA; personal data protection

check for updates

Citation: Pantelic, O.; Jovic, K.; Krstovic, S. Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations. *Sustainability* **2022**, *14*, 5015. https://doi.org/10.3390/su14095015

Academic Editor: Miltiadis D. Lytras

Received: 19 February 2022
Accepted: 18 April 2022
Published: 22 April 2022

1. Introduction

Today, there is almost no organization that does not exist in the online world. Various organizations collect user data to analyse user behaviours, attitudes, and habits. User data affects a company's business and determines the direction of further development of a company. With the evolution of the Internet, the exchange of digital information has become more accessible. The future of digitalization is personalization, and the purpose of organizations should be to provide the individualization of user searches. After a user accesses a website, certain information is placed on their device in the form of a text message. This information, which recognises the user, is called a cookie. Cookies are one of the new concepts in technology that have made a big difference in the use of the Internet. Both the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) require an adequate context for processing personal data. GDPR is the EU's data protection and security law [1], while the CCPA is a law covering the use of California citizens' data [2]. It is important to delineate the difference between personal data and non-personal data in the scope of application of these documents.

There is a significant economic impact from data that is not personal on its face but can be considered as personal if needed, as well as an impact on the spectrum between data that is clearly personal and data that is clearly anonymous.

The development of new technologies and the introduction of changes in the appearance of the Internet aim to improve user activity. In addition to user convenience, with the development of the digital world, many organizations are implementing better online performance. The cookie contains two important pieces of data: the user identifier and important information related to the user. Cookies usually contain the name of the server from which the cookie was sent, the duration and the value [3]. The server uses this value for collecting user data in order to recognize the user during the next session [4]. Usually, only the server that sends the cookie can interpret it [5]. Cookies enable service providers to offer features relevant to both them and end-users. Information collected in this manner can be used for creating new offerings or targeted ads or improving existing products and services [6]. Before cookies, each visit to the specific webpage from a specific user was treated as the first visit [7]. If cookies are handled properly, they do not pose a danger and cannot transmit viruses or malware. Otherwise, viruses and malware can be transformed into cookies. An example of manipulating cookies is a supercookie, which can be a security issue, or a zombie cookie, which can be created after it has been deleted. There are different categories of cookies. Some cookies are mandatory—without their presence, it is impossible to access the basic functionalities of the website—while some of them are optional and exist to improve the user experience. The part of this paper that deals with different categories of cookies shows which factors are considered when choosing them. Data privacy management software is also considered, along with its collaboration with cookies. Data privacy management software simplifies protecting data and enables enterprises to store sensitive data in compliance with the law.

Privacy protection is one of the most important areas of information technology, with application in various spheres of business. Tracking the movement of cookies can endanger the privacy of users in different situations of illegal use, which is not their primary purpose. Internet privacy is a part of computer privacy, and it is of great importance at the moment when the user decides to appear on the Internet. Each user aims to protect their data. In this area, two important personal data protection regulations are considered: the GDPR and the CCPA. An important part of the chapter will be dedicated to the technological goal of introducing the principles of data protection as well as the technological challenges that have arisen with the adoption of these provisions. The most important goals in this paper are (1) the safe handling of cookies; (2) opportunities to improve existing integrations; (3) how to bridge the gap created between functional GDPR and CCPA requirements and technical capabilities. It is important to identify what dangers exist when using cookies, how traps can be avoided and how they can be used ethically. The main problem is not digitalization and its development, but what people plan to do with it.

2. Materials and Methods

In order for the outcome of this research to be meaningful, it was essential to first seek out foundational knowledge, such as legal outlines, specifications, and technical aspects of cookies and data privacy. Legal documents defining GDPR and CCPA, literature describing cookies, and credible websites were key for this step.

A sample of websites was selected in order to gauge the alignment of the legal outlines with the actual state of affairs. It was important that the selected websites are visited by a large demographic, preferably a global audience, that they are from different regions, such as the EU and the USA, and that they can be classified into a single industry, in order to control for that factor. This way, it can be gauged whether websites behave in accordance with the local laws and also how website groups from different regions compare among themselves. For this reason, news outlets from the USA and the EU were selected.

The final step was to seek out the most used privacy management software tools and discover how they handle cookie management, user privacy and transparency.

3. Theoretical Background

There are several different theories about how cookies were created. Cookies were created to give a better experience to the user. Web services were not able to store a state. For example, it was impossible to implement a shopping cart, or an interactive map [8]. One of the theories is that a web developer, Lou Montulli, wanted to collect information and used a text document for that purpose. In July 1994, the twenty-four-year-old programmer came up with a new concept. The original information-gathering solution required a file that could be placed on each visitor's computer to monitor what had been done on a particular website. This solution was originally called a permanent client object. In some earlier research, when machines sent small chunks of code, developers called the chunks magic cookies. Montulli considered cookies to be the descendants of magical cookies, so the name "cookie" was assigned accordingly [9]. This concept represents a major milestone, not only in Internet access but in the entire science of computing. The original description of cookies can be found on Netscape's website. Especially important in the technical document prepared by Montulli was that the connection between cookies and the concept of privacy had never been mentioned before [3]. Figure 1 shows the graphical representation of the cookie development timeline, with major milestones included.

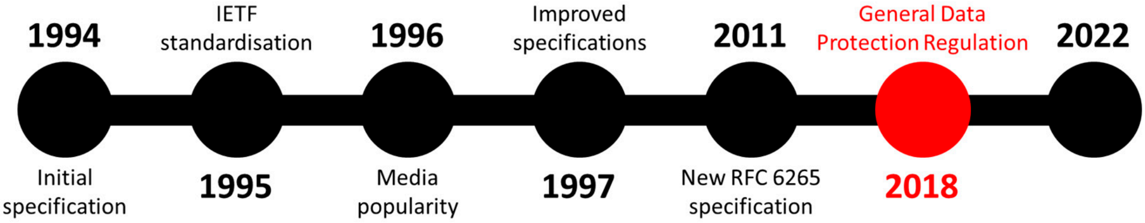

Figure 1. The graphical representation of the cookie development timeline.

In today's world, mechanisms for monitoring users without their knowledge have become increasingly prevalent, and thus should be regulated by laws [10]. Users can access the website through a web browser, after which a text document called a cookie can be created. The device stores text files locally, and the data is forwarded back to the website. In the future, when a user accesses the website again, cookies will store the data and allow the site to manage it [11]. This is how insight into the previous user activity is created. Depending on the text file that is stored, a website can act in a variety of ways. For example, each user can be recognized as a repeat visitor and may receive customized service. The major goal of storing user data and monitoring user activities is to improve the website and the user experience. On one side, there is no need for privacy concerns if personal information is not processed. On the other hand, it is important to understand users' behaviour when they visit a website [12]. For each user, there is a specific set of data points that connects them with cookies. When a user visits a website, their identification can be set to, for example, "User 1". The next time the user accesses the same website, they will be recognized based on their identification. The two important pieces of data, the user identifier and important information related to the user, can be represented within just one attribute or a series of attributes [13]. Figure 2 shows a simplified representation of the cookie–server communication.

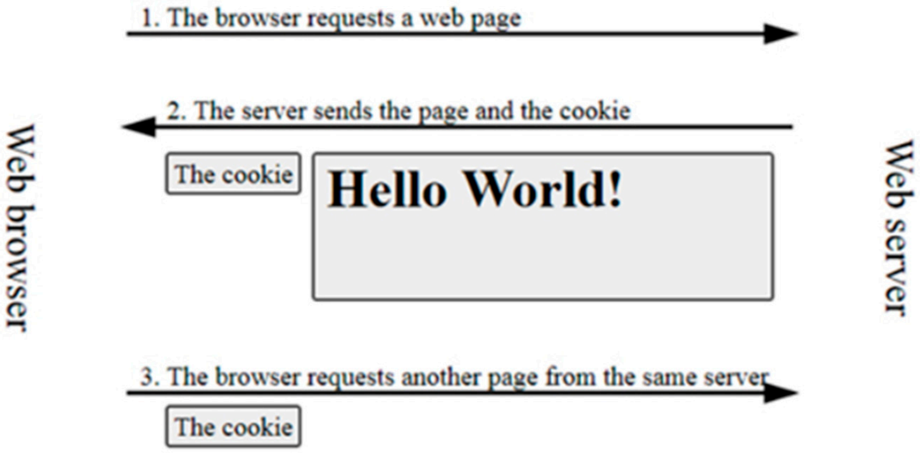
1. The browser requests a web page
2. The server sends the page and the cookie
The cookie
Hello World!
Web browser
Web server
3. The browser requests another page from the same server
The cookie

Figure 2. A simple representation of the communication between the cookie and the server [13].

One of the most important classifications of cookies is based on the origin and destination. As shown in the Table 1, cookies can be classified into first-party cookies, which are created by the visited domain, and third-party cookies [14]. It is considered that first-party cookies cannot compromise user privacy. On the other hand, third-party cookies are created by third-party entities, and they can cause security risks [15].

Table 1. First-party cookies and third-party cookies.

Parameters	First-Party Cookies	Third-Party Cookies
Implementation	Implementation by the website owner	Implementation through third-party servers
Availability	Only the domains that have created them have access	Any website that implements third-party cookies has access
Web browsers	Supported by all search engines	Supported by all search engines

As can be seen in the Table 2, there are five different types of cookies depending on duration and purpose. Session cookies are temporarily collected information that can be removed immediately after closing the web browser. All data collected by this cookie are used to identify the session. A session cookie exists in memory while the user navigates through the site. This cookie usually disappears after closing the browser, and because of that, it can also be called temporary [16]. The original idea for persistent cookies came from Montulli's 1998 patent and the concept of adding client-side memory to a stateless Internet protocol [17]. Persistent cookies are placed on the user's device to make user data storage faster. This helps website owners and users to have a better experience on the website [18]. Persistent cookies allow websites to remember data and activities that will be used in the future. The main difference between persistent cookies and session cookies is the expiration date. If the cookie does not contain an expiration date, it is considered to be a session cookie. In addition, session cookies present a lower privacy reduction [19]. Otherwise, they are considered persistent cookies. The concept of mandatory cookies implies that access to certain information is essential. Strictly mandatory cookies must be presented as primary, and they cannot be turned off. They do not require consent from the visitor, but the visitor should still be informed about the purpose of the necessary cookies on the site [20]. They are typically first-party cookies, but not all first-party cookies are strictly mandatory cookies. Performance cookies collect new ideas and track website visitors. They collect users' data through the site and use that data to improve the website's performance. Performance cookies show the users' communication with the website, without identifying them as individuals. Thus, performance cookies are usually set as targeting cookies [21]. All data that are aggregated anonymously should provide website owners with statistical information about their site. One of the main features of functional cookies is to provide users with a customized user experience. Functional cookies allow websites to remember user data, such as the username, region settings, or selected language. They help website owners to completely personalize the features, and they are usually a combination of first-party, third-party, session, and persistent cookies. Tracking user habits enables the development of a targeted profile for the user and the display of the desired ad that is relevant to the selected user. Typical uses of marketing cookies are retargeting, internet advertising, and social networks. They are controlled mainly by advertising partners. One of the most popular types of advertising is behavioural advertising. Behavioural advertising allows a website to remember a user's pattern, and when the user returns, the site will serve adequate content [22].

Table 2. Comparative analysis of cookies depending on duration and purpose.

Type	Duration	Purpose
Session cookie	It is deleted after closing the browser	Tracking
Persistent cookie	Long duration	Mostly for online marketing
Supercookie	Long duration	History and habits
Secure cookie	Long duration	The connection type should be HTTPS
Zombie cookie	Long duration	A cookie can be recreated

Tracking can be used for a wide range of purposes. Thus, collected data can be sold to other parties. The primary idea of web tracking was developed to increase sales profit [23]. A secure cookie is used for storing information and transferring it across security connections. One of the main advantages of this type of cookie is maximum security in data transfer. A secure cookie always has the secure attribute activated, and it is transmitted with encrypted connections [24]. The secure attribute is not the only security mechanism for cookies—there are also HttpOnly and SameSite attributes. "Supercookie" is the name for a cookie concept that falls into the category of user tracking technologies. The original idea of supercookies was to monitor user behaviour and habits [25]. However, the mechanism of indelible cookies has led to the increasing use of supercookies for illegal purposes. A zombie cookie is automatically recreated after deletion. It can be placed in several places on the user's device, which makes it very difficult to delete. Most often, these cookies are used for web analysis and marketing. Zombie cookies allow the web tracking companies to obtain information such as previous unique user IDs and continue tracking [26]. Flash cookies were developed by Macromedia Flash, and the first Flash cookie-enabled Flash player was Flash Player 6. They were not removable until September 2006 [27]. A Flash cookie is also known as a local shared object, and this text file is stored in a separate directory. Thus, users are usually unaware of them and sometimes may not know what files to delete to remove them [28].

Data protection laws require website owners to comply with data protection measures. There has been a need for new types of modals whose purpose is to inform users about how their data is used. Specific modals that appear on websites and require approval from the user for cookies are cookie banners. Their purpose is to inform the user about how their data is used and to obtain user consent for data collection [29]. Some studies have shown social framing to be an important behavioural nudge, reducing cookie acceptance in the minority social norm condition [30]. Users have a choice—in the case they decide not to accept cookies, their data will not be processed. Companies that process any kind of user behaviour, regardless of whether through services or products, must comply with regulatory measures. This means that the GDPR applies to almost all services that affect EU citizens [31]. Parameters that are observed for considering the compliance of cookie banners with the GDPR are the following [32]:

- Cookies Accept Button—This button allows the user to choose which category of cookies to accept;
- Use of cookies—The pages must provide the user with information on the purposes for which the data will be used;
- Information about sharing data with third parties—It must be explicitly stated whether third parties use users' data or not;
- Link to the privacy policy or cookie policy page—It is mandatory to have a description of cookies and acceptance conditions on the cookie policy.

Parameters that are observed for considering the compliance of cookie banners with the CCPA (California Consumer Privacy Act) are as follows:

- Use of cookies—The user should be informed about cookies and if the website owners share the information with third parties;
- Cookies Accept Button—One of the most important differences between GDPR and CCPA is that websites can drop some cookies before the user clicks the accept button;
- Do not sell button—CCPA requires companies to give customers the option to opt-out of selling personal information.

Different laws try to protect personal data using cookie banners in accordance with their rules. In any situation when the website uses user data and it is unnecessary for the operation of the site, a cookie banner is considered to be a mandatory part of the site [33]. A cookie policy is a special report about what cookies the website is using and for which purposes. In today's world, a cookie policy is in coordination with modern browsers, and some tracking problems can be resolved easily with a basic option, for example, Firefox's "Never accept third party cookies" [34]. The privacy laws require the website owners to have a cookie policy as a mandatory section of the website, and it is up to them to decide whether this will be inside the privacy policy section or as a separate cookie policy section. The reason for attaching a cookie policy to the privacy policy section is that cookies provide the ability to track users, and therefore there is a potential risk of compromising privacy [35]. A cookie policy complies with the CCPA and the GDPR if it meets the following conditions [36]:

- It is clearly indicated what types of cookies are placed;
- It provides information about keeping cookies in the browser;
- It provides information about data collected from users;
- It provides information about sharing users' data;
- It provides information on how to change cookie-related settings.

An important question for discussion is how to connect a cookie policy and a privacy policy, so they can be consolidated. There is a problem with constantly changing cookies; the cookie policy needs to be up to date. One of the safest ways to ensure complete control over cookies is to implement a software solution for cookies that complies with cookie law requirements and thus ensures that the cookie policy will always be integrated with the cookies set on the website. Several free solutions can be found online, which can help website owners meet the legal criteria.

Privacy management software serves to increase the efficiency and accuracy of the privacy process through the automation of complex activities, such as privacy impact assessments, data protection impact assessments, and data mapping [37]. Clients who choose to use the software can ensure protection against legal risks and compliance with privacy laws. Some of the most popular privacy management software is:

- OneTrust;
- Cookiebot;
- Crownpeak Universal Consent Platform;
- Piwik PRO Consent Manager, TrueVault;
- Informatica Data Privacy;
- AuraPortal GDPR Accelerator;
- Cookie Consent by Insites;
- IBM Data Risk Manager;
- AvePoint Compliance Guard.

Privacy management software solutions enable complete information management, the ability to create data maps, and registers. They have a simple design, great adaptability to customer needs, and a simple mechanism for scanning cookies. The biggest disadvantage of using software is the process of synchronizing with other tools. In the case that the configuration of this solution is not set up correctly, it can take a long time to scan websites. The advantages of using privacy management software are [38]

- Real-time monitoring;
- Third-Party Security Risk Assessment Tools;
- Consent-Based;
- Taking into account a wide range of laws.

The data management platforms have some common features and some special functions that depend on the application. Privacy policies such as the CCPA and GDPR require user consent and oblige platforms to secure the data. Therefore, it is convenient for companies to implement a complete solution. Companies should provide more choices for consumers [31]. A lot of programs include standards for personalized advertising and marketing. In addition, companies are using non-cookie technologies, like device fingerprinting, which are harder to control. The most important goal a business has is the trust of its customers, and the trust should be in privacy protection at every level.

Throughout history, data privacy has always been important to people. In 1877, Thomas Edison was putting the finishing touches on his invention: the phonograph. This would lay the foundation for the record player, and these devices could both record and play back audio on paper or malleable metal tapes or tubes. In 1888, George Eastman released the Kodak Camera, the first commercially available camera. People began to question the use of these new devices. In 1890, a 42-page article called “The Right to Privacy” was published in the Harvard Law Review. This is one of the first known papers to raise the issue of consent when being photographed or recorded. Society commented on the importance of privacy long before the invention of cookies.

4. Technical Aspects of Cookie Implementation

At the very beginning of the creation of cookies, not much was known about them. They were placed by default, so users were not aware of their presence. They attracted a lot of media attention after the publication of an article in The Financial Times about how they can affect users’ privacy. After cookies became a major topic in the media, the first formal integration of cookies was done by the IETF (Internet Engineering Task Force). The development of the Internet has greatly influenced the communications of many business organizations. Under the influence of information and communication technologies, new modalities for collecting data from users have emerged. The need to view the user as an individual, and not just as a part of a group, has fostered the emergence of the concept of cookies. Many people today use the Internet for various purposes, but they are still not aware of the existence of cookies as a special concept that intends to help content on the Internet reach a wider audience. The average user does not know much about caching, log files, and how data is transferred between their personal computer and a web server. However, all users require that their unique data stay secure.

Cookies are one of the technologies that have made a big difference in the use of the Internet. The implementation of cookies affects the increase of awareness about the devices that are used, which data is collected, and for which purposes. For these reasons, national laws require website owners to inform the user about the data collection.

An example of setting cookies on the client side:

```
document.cookie=‘name=testCookie’
```

The lifetime of the cookie:

```
document.cookie=‘name=testCookie;expires=Mon,26Mar2020 17:04:05 UTC’
```

Example of path setting:

```
document.cookie=‘name=testCookie;path=“/”‘
```

Domain setup:

```
document.cookie=‘name=testCookie;domain=“test.com”;’
```

By adding the Secure parameter, the cookie can only be securely transmitted over encrypted HTTP connections:

```
document.cookie=‘name=testCookie;Secure;’
```

name = VALUE—The name is a mandatory cookie attribute and should not contain characters such as semicolons, spaces, or commas.

expires = DATE—This attribute is optional and represents the duration of cookies. Once the expiration date is reached, the cookie will disappear.

domain = DOMAIN_NAME—The default domain value is the host name of the server that generated the cookie response.

path = PATH—This attribute is optional, and it is used to specify subsets of URLs in domains for which the cookie is valid.

The example of setting cookie in JavaScript:

```
    setCookie: function (name, value) {
    var date = new Date();
    date.setTime(date.getTime()+this.cookieTimeout); document.cookie=name+’=‘
+value+’;expires=‘+
    date.toGMTSting()+ ‘;path=/’;
}
```

The example of the delete cookie function in JavaScript:

```
deleteCookie: function (name) {
var hostname = document.location.hostname.replace(/ˆwww\./, “),commonSuffix=‘;expires=Thu, 01-Jan-1950 00:00:01 GMT; path=/’;
document.cookie = name + ‘=; domain=.’ + hostname + commonSuffix;
document.cookie = name + ‘=‘ + commonSuffix;
}
```

Some of the most popular cookies are the Google Analytics cookies. Google Analytics was developed to provide information about user behaviour. Behaviours include everything involved in the journey they take through the site [12]. Implementation of the asynchronous version of the analitics.js library allows web browsers to pre-load the tracking code. By clicking on the accept button for this type of cookie, the cookies are implemented. For example, if the user works with Google Chrome, a tab for cookies is built directly into the Google Developer Tools.

```
    <script>
    (function(i,s,o,g,r,a,m){i[‘GoogleAnalyticsObject’]=r;i[r]=i[r]||function(){
    (i[r].q=i[r].q||[]).push(arguments)},i[r].l=1*new Date();a=s.createElement(o),
    m=s.getElementsByTagName(o)[0];a.async=1;a.src=g;m.parentNode.insertBefore(a,m)})(window,document,’script’,’https://www.google-analytics.com/analytics.js\T1\textquoteright,\T1\textquoterightga’);
    ga(‘create’, ‘UA-XXXXX-Y’, ‘auto’);
    ga(‘send’, ‘pageview’);
    </script>
```

Different browsers allow users to manage cookies and configure cookies in different ways. Users have the option to change their privacy settings in accordance with their needs. One of the biggest questions discussed is the need to disable cookies in a browser. There is no universal answer, because it depends on the user's preferences. Different browsers give different choices to disable cookies. The most common options that browsers provide for managing cookies are (1) users fully accept or block cookies; (2) the cookie manager helps the user in selecting and deleting cookies. In the unknown conditions of accepting cookies by all browsers, a new task for the engineering working group was developed. Their goal was to establish a formal cookie specification. There was an attempt to lay down a condition banning third-party cookies, but browser manufacturers nevertheless continued to allow third-party cookies to be tracked. Today, the engineering working group accepts the use of cookies and all the risks that arise during their use, but full responsibility is placed on the team of web browser developers. Some of the browsers have specific functionalities, like ETP (Enhanced Tracking Protection), made by Mozilla, which can be used against cookies. This anti-tracking concept keeps the identity of the user secret by blocking cookies that track the user online by collecting sensitive data.

In December 2010, the FTC published a report in which they demanded search engines introduce the DNT (Do Not Track) function. This concept gives users the ability to avoid online tracking. The DNT header can be used to disable individual user tracking [19]. It can have the value 1 in the case the user does not want to be tracked, 0 in the case the user agrees to be tracked, or null in the case the header is not sent. "Do Not Track" failed primarily because companies had no reason to adopt it and most of them ignored it. Data collection requirements established by privacy legislation gave a new point of view to the industry and digitalization. First, the Electronic Frontier Foundation (EFF) started work on a DNT policy of its own, based on stronger privacy criteria. EFF's DNT policy requires that users who have turned on the DNT signal are not tracked without being informed at the beginning. If DNT is turned off, it has strict limitations on what data can be collected. The DNT policy started in August 2015, when the W3C published two proposed standards, the Tracking Preference Expression (TPE) and Tracking Compliance and Scope (TCS). At the same time, while the developing DNT, the European Union passed GDPR, and California raised CCPA, which were consolidated with the DNT mechanism. This brings the important challenge: the digital ecosystem must be completely legal to develop user trust and good practices in the industry.

5. Legal Aspects of Cookie Implementation

Tracking users online can compromise user privacy. The primary use of cookies is not illegal. Websites sometimes want to personalize the user experience and, in their desire to offer the best content, achieve the opposite effect. Cookies do not pose a risk to the user and the computer if managed properly. Personal data are generated by collecting information from users, which is obtained through various monitoring activities. The data are not collected automatically by cookies. Privacy refers to the right of an individual to manage his or her own data and that no one may gain unauthorized access to data that the user considers personal. It is necessary to decide which parts of the data will be stored in the cookie, as it can be one of the potential security risks of working with sensitive data. The right to privacy is one of the most important human rights, and technology is evolving toward improving protection measures. However, market share has also developed in the opposite direction, which violates the right to privacy.

Data that can be related to someone's identity are considered personal data. Users can consciously or unconsciously leave personal data in the online world, and their data can be processed in an ethical or unethical way. A task that involves any action related to personal data, such as collecting, storing, and tagging, also involves processing that data. The processing of personal data includes any active or passive action performed on personal data. Therefore, any processing of personal data is considered in accordance with the law [39]. Consent is one of the most well-known GDPR bases and also one of the most well-known bases in handling cookies. According to the GDPR, consent is given by a certain confirmatory action that signifies the voluntary user consent for personal data processing. The main characteristics of consent are [31]

- Existence of consent withdrawal option,
- Consent must be specific;
- Consent must be classified;
- Consent must be unambiguous;
- The operator must prove that the person gave consent.

5.1. General Data Protection Regulation

The aim of this regulation was to set consistent standards for the processing of personal data within the European Union. The GDPR considers personal data to be any data that can be used to uncover the identity of a user [40]. Since the enactment of this regulation, web services have taken on an additional dimension of data processing. If organizations deal with processing personal data, they must have a legal basis for their processing and ensure the transparency of their collection procedures [35]. The security of users on the Internet is basically the goal of harmonizing cookies with the GDPR. Every website that uses cookies should inform its users about their use. Everyone should be informed about what data is used, for how long, and where it is stored. It is possible to prohibit the use of data and request its deletion at any time. Proper processing of user data is a priority, and thus any non-compliance with the law is sanctioned. Compliance with regulations requires

- User consent;
- Information for each category of cookies;
- Purpose and use of cookies;
- Ability to delete data;
- Documented user consent.

5.2. California Consumer Privacy Act

The California Privacy Act came into force in January 2020, and it is the first US law of its kind. This data privacy law regulates how businesses around the world may process the personal data of California residents [2]. It was introduced to protect the privacy of citizens living in California. Companies are required to provide consumers with detailed information on what they do with their data and must have the ability to give consumers the choice to opt out of sharing their data. CCPA requires

- Annual revenue of 25$ million or more;
- Personal information for more than 50,000 users;
- More than half of the annual revenue from the sale of users' personal data.

One of the biggest differences between the CCPA and the GDPR is that the CCPA focuses on consumers from California, while the GDPR seeks to create certain privacy for the entire EU. According to the CCPA, an organization does not need the prior consent of users before processing their data. Compliance with the law is a process that requires the constant improvement of activities and the implementation of best security practices. The effective enforcement of measures includes restricting access to data, deleting inadequate data, monitoring personal data to maintain security, and constantly updating data management licenses.

5.3. Technological Challenges of Aligning Cookies with GDPR and CCPA

Computers have completely changed the ways of storing and collecting information. Not only has computer technology increased the volume of information collection, but it has also enabled the collection of new types of information. Today, it is impossible to eliminate or even limit the collection of personal data. This is exactly why it is challenging to define laws that balance the privacy rights of users with the needs of the community to gather information.

The technological challenges can be discussed from the three different aspects:

- From a user perspective, it is necessary to consider the differences at the micro-level of everyday user practices between different user groups;
- The technical aspect must be in tune with new monitoring techniques;
- The privacy policy should connect technology and users by dealing with transparency.

After legal regulations were introduced, users were given greater security that their data would be safe and stored adequately. However, for business owners, storing data is a real challenge. Business owners must know when to revise databases, to ensure that they comply with all provisions. It is necessary to store structured data because each individual may request insight into the details of the data, which must be presented to the user in an understandable form. The GDPR and CCPA have led data controllers to follow strict approaches in selecting data processing technologies. The GDPR and CCPA have an enormous impact on the development of future technologies. Companies that build their brand in compliance with the law have a strategic opportunity to achieve a competitive advantage in the data world. Technology companies in the global market are encouraged to make significant efforts to ensure that their data, products, and services comply with legal requirements.

6. Results

The foundation of this paper is the problem of transparency. The most important research questions that were used when analysing the web pages are

- Q1: Does the site have a cookie notification?
- Q2: Does the site have a privacy policy?
- Q3: Does the site implement privacy management software?
- Q4: Is the site functional if cookies are disabled?
- Q5: Is the cookie policy link separate from the privacy policy link on the homepage?

Figure 3 shows the research questions were made based on the GDPR and CCPA requirements and should act as a measure of how well the websites fit the legal requirements. The test websites were chosen based on the criteria outlined in Materials and Methods, and they represent websites with a large number of visitors that could benefit from utilizing cookies and belong to the same industry, so as to control for that factor. Three online newspapers from the US were used for the research: USA Today, The Wall Street Journal, and The New York Times, as well as two online newspapers from the UK and the EU: The Guardian and The Irish Times.

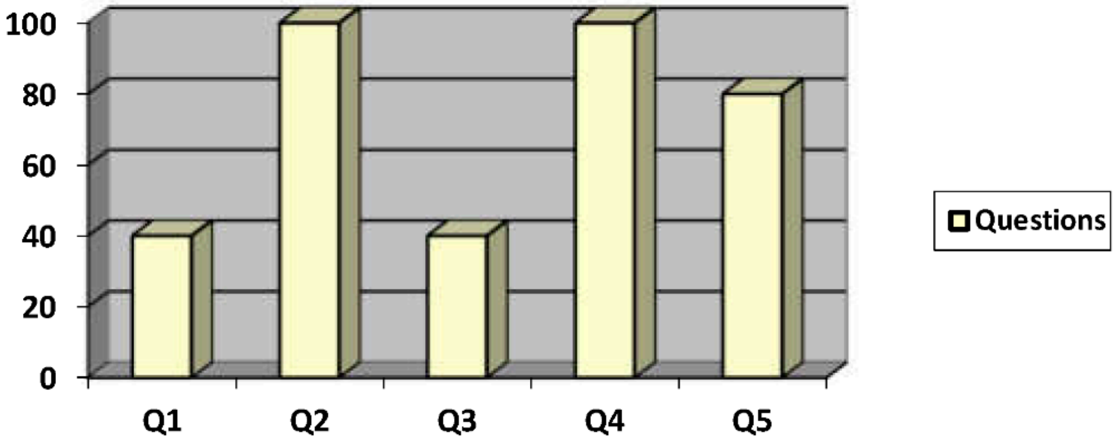

Figure 3. Analysis of the research questions.

One of the most important rights is to give users accurate information. Therefore, before collecting data from users, all media must present a range of information about the data they plan to collect for certain purposes, and to achieve the principle of transparency. In order to avoid doubts among users, it is necessary to adequately present each of the aspects of personal data processing [31].

From Table 3, we can see that USA Today and The Wall Street Journal have explicitly defined links for the Cookie policy on the homepage. This is one of the biggest advantages for the users as it is easier for them to check the important information about cookies. In addition, USA today has privacy management software (OneTrust) implemented, and accurate information about cookies is shown in the form of the cookie banner.

Table 3. The analysis of the different online newspapers.

Websites	Q1	Q2	Q3	Q4	Q5
USA Today	No	Yes	Yes	Yes	Yes
Wall Street Journal	No	Yes	No	Yes	Yes
New York Times	No	Yes	No	Yes	No
Guardian	Yes	Yes	No	Yes	Yes
Irish Times	Yes	Yes	Yes	Yes	Yes

For example, OneTrust is a privacy management software solution created to help companies align their business with the law. It enables complete information management and data map and registry creation, meaning it is exceptionally useful for teams managing private user data. Upon scanning cookies, it assigns them to specific categories, which the user can activate or deactivate [41]. Another example, Cookiebot, also screens a website to verify its compliance with the law and generates a report based on the findings [42].

7. Conclusions and Discussion

Cookies do not represent harm to the user and the computer by default. Personal data is generated by collecting information from users, which is obtained through various monitoring activities. The data is not collected automatically by cookies. If users want to be in the digital world, it is important for them to first learn about digitalization and then decide if sharing personal information is safe or not. It is necessary to decide which parts of the sensitive data will be stored in the cookie, as this can be one of the potential security risks.

The principles of privacy protection, according to all international principles, require the application of strong security measures for protecting personal data. Organizations that adhere to the principles will have a reduced number of security errors. Fewer security errors mean that the business does not lose the trust of its users. Organizations that do not enforce privacy protection face large fines as well as the loss of users and business collaborations. The digital world is constantly growing, so it is necessary to develop online media accordingly. With the introduction of cookies, new tasks and obligations were created, both for media producers and media users.

Cookies are one of the most useful technologies for collecting personal data, and from the point of the CCPA, they are defined as unique identifiers that need to be included in the defined law. What distinguishes the CCPA from the GDPR is its focus on consumers from California; the GDPR seeks to create a certain kind of privacy automatically for the whole of the EU. According to the CCPA, an organization does not need the prior consent of users before processing their data. Consent is one of the most well-known GDPR bases and also one of the most well-known bases for handling cookies. According to the GDPR, consent is given by a certain confirmatory action that signifies the voluntary consent of the user to the processing of personal data. The security of users on the Internet is the major goal of cookies coordination with the GDPR and CCPA regulations. Thus, organizations must harmonize their business with the GDPR and CCPA regulations. It is very important to realize that cookies are not viruses and do not represent programs through which security attacks are carried out on users. Users enter the information they want. As long as the user decides to leave any data, they remain anonymous. Cookies are primarily intended to complete the user experience and to make access to various sites on the Internet more efficient [13]. Every individual who uses the Internet, above all, should be informed about their privacy and how they can protect it. It is necessary to see the advantages of accepting all cookies when accessing a particular website, as well as the disadvantages. The conscious presence of the user when online allows them to collect and see all the information related to cookies and then decide if it will be helpful. Many solutions help the user evaluate information and protect privacy. However, the safest way to ensure protection is to educate users and make them technologically literate. Edward Snowden explained this by saying "arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say". In today's world, most websites comply with the law, but the cookie policy is often unclear to users, who may completely ignore the content of the privacy policy because of the lack of understanding. People who create the content and are fully focused on the adequate presentation of the purpose of cookies try to avoid the growth of the population that rejects and regularly deletes cookies. Data privacy in correlation with cookies relates to how a piece of information should be handled. Based on data importance, for example, we do not have any problem sharing our name with someone in the process of introducing ourselves, but there is other information we do not want to share. In addition, a person has the option to choose to revert the data or to change the data. This should be considered a fundamental human right, and data protection laws exist to guard that right. Data protection laws around the world give individuals power over the data and the right to know how their data is being used, by whom and why. From a business perspective, protecting personal data can have multiple positive impacts on the organization and customers' expectations, and from the user's perspective, privacy should be considered a fundamental human right.

An intelligent algorithm can be developed for the benefit of the end-user. This algorithm would be based on the research questions outlined in Section 6. It would follow a logical series of steps in order to determine the security and privacy status of a website. The following steps are recommended:

1. Verify whether the website has a cookie notification. If yes, continue to Step 2.

2. Verify whether the website has a privacy policy. If yes, continue to Step 3. Otherwise, verify whether the website has a cookie policy.
3. Verify whether the website has built-in privacy management software.
4. Verify whether the website is operational when cookies are blocked.
5. Verify whether the privacy and cookie policies are on separate links. Many websites bundle the privacy and cookie policies, which is not in the user′s best interest, so the modern tendency is to split them.
6. Gauge the website's success by counting up all steps where the website successfully passed.
7. Allow or restrict access depending on whether the website passed a predefined threshold. For example, if the website met three or more out of five criteria, it is deemed safe.

This algorithm can be implemented in a user-friendly way, such as a chatbot or a browser extension, which could be used by people who are not technical experts and be distributed to wide audiences.

Future work will be focused on further calibrating the algorithm and automating it through the aforementioned chatbot or browser extension. In order to calibrate the algorithm, more website data will be collected and analysed. Based on the results, the algorithm will be expanded with sub-steps and possible pondering based on the perceived importance of each factor. The development of the browser extension or chatbot will be started afterwards.

Author Contributions: Conceptualization, O.P. and K.J.; methodology, O.P. and K.J.; software, K.J.; validation, O.P., K.J. and S.K.; formal analysis, K.J.; investigation, K.J.; resources, O.P. and K.J.; data curation, K.J.; writing—original draft preparation, K.J.; writing—review and editing, O.P., K.J. and S.K.; visualization, K.J.; supervision, O.P.; project administration, O.P., K.J. and S.K.; funding acquisition, O.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. General Data Protection Regulation (GDPR). Available online: https://gdpr-info.eu/ (accessed on 5 April 2022).
2. California Consumer Privacy Act (CCPA). Available online: https://oag.ca.gov/privacy/ccpa (accessed on 5 April 2022).
3. Kristol, D.M. HTTP Cookies: Standards, Privacy, and Politics. *ACM Trans. Internet Technol.* **2001**, *1*, 5–16. [CrossRef]
4. What is a Cookie? Available online: https://www.techtarget.com/searchsoftwarequality/definition/cookie (accessed on 6 April 2022).
5. All about Cookies. Available online: https://www.allaboutcookies.org/cookies/ (accessed on 6 April 2022).
6. Spanish Data Protection Agency. *A Guide on the Use of Cookies*; AEPD: Rome, Italy, 2019.
7. What Are Cookies? Available online: https://cookiecontroller.com/what-are-cookies/ (accessed on 6 April 2022).
8. Eijk, R.J. *Web Privacy Measurement in Real-Time Bidding Systems. A Graph-Based Approach to RTB System Classification*; Leiden University: Leiden, The Netherlands, 2019; pp. 37–38.
9. Giving Web a Memory Cost Its Users Privacy. Available online: https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html (accessed on 10 January 2022).
10. Zimmerman, R.K. The Way "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century. *N.Y.U. J. Legis. Public Policy* **2001**, *4*, 441–444.
11. What Are HTTP Cookies. Available online: https://www.addthis.com/academy/what-are-http-cookies/ (accessed on 12 February 2022).
12. Ma, H. Tech Services on the Web: Google Analytics. *Tech. Serv. Q.* **2019**, *30*, 119–120. [CrossRef]
13. What Is a Website Cookie? How Cookies Affect Your Online Privacy. Available online: https://www.makeuseof.com/tag/whats-a-cookie-and-what-does-it-have-to-do-with-my-privacy-makeuseof-explains/ (accessed on 22 January 2022).
14. Yue, C.; Xie, M.; Wang, H. An automatic HTTP cookie management system. *Comput. Netw. Int. J. Comput. Telecommun. Netw.* **2010**, *10*, 2182–2183. [CrossRef]

15. McStay, A. An analysis of the Cookie Directive and its implications for UK behavioral advertising. *New Media Soc.* **2013**, *15*, 598–600. [CrossRef]
16. Browser Cookies: What Are They & Why Should You Care. Available online: https://www.whoishostingthis.com/resources/cookies-guide/ (accessed on 13 January 2022).
17. Berghel, H. *Toxic Cookies*; University of Nevada: Reno, NV, USA, 2013; Volume 46, pp. 104–105.
18. Persistent and Non-Persistent Cookies in ASP.NET. Available online: https://codeasp.net/blogs/asp-net/6235/persistent-and-non-persistent-cookies-in-asp-net (accessed on 23 December 2021).
19. Cofone, I. The way the cookie crumbles: Online tracking meets behavioural economics. *Int. J. Law Inf. Technol.* **2017**, *25*, 15–20. [CrossRef]
20. Cookie Notice. Available online: https://www.independent.co.uk/service/cookie-policy-a6184186.html (accessed on 23 December 2021).
21. Cahn, A.; Alfeld, S.; Barford, P.; Muthukrishnan, S. *An Empirical Study of Web Cookies*; International World Wide Web Conferences Steering Committee: Geneva, Switzerland, 2016; pp. 894–895.
22. Bennett, C.S. Regulating Online Behavioral Advertising. *John Marshall Law Rev.* **2011**, *44*, 491–492.
23. Bujlow, T.; Carela-Español, T.; Solé-Pareta, J.; Barlet-Ros, J. Web Tracking: Mechanisms, Implications, and Defenses. *arXiv* **2015**, arXiv:1507.07872. [CrossRef]
24. Secure Your Cookies (Secure and Http Only Flags). Available online: https://blog.dareboost.com/en/2019/03/secure-cookies-secure-httponly-flags/ (accessed on 13 February 2021).
25. What Are Super Cookies and How to Remove Them. Available online: https://www.comparitech.com/identity-theft-protection/supercookie/ (accessed on 23 December 2021).
26. Zombie Cookies: What They Are and How to Disable Them. Available online: https://www.esozo.com/zombie-cookies-what-they-are-and-how-to-disable-them/ (accessed on 12 December 2021).
27. Challenges for Online Privacy: The Use of Cookies in Social Media. Available online: https://www.emeraldgrouppublishing.com/archived/learning/management_thinking/articles/cookies.html (accessed on 10 February 2022).
28. Tene, O.; Polonetsky, J. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minn. J. Law Sci. Technol.* **2012**, *13*, 292–294. [CrossRef]
29. Cookie Banners and Accessibility. Available online: https://uxdesign.cc/cookie-banners-and-accessibility-d476bf9ee4fc (accessed on 12 December 2021).
30. Personality and Social Framing in Privacy Decision-Making: A Study on Cookie Acceptance. Available online: https://www.frontiersin.org/articles/10.3389/fpsyg.2016.01341/full (accessed on 17 January 2022).
31. Krivokapić, D.; Adamović, J.; Tasić, D.; Petrovski, A.; Kalezić, P.; Krivokapić, Đ. *Vodič kroz Zakon o Zaštiti Podataka o Ličnosti i GDPR Tumačenje Novog Pravnog Okvira*; SHARE Foundation: El Dorado, AR, USA, 2019; pp. 13–42.
32. Matte, C.; Bielova, N.; Santos, C. Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework. In *IEEE Symposium on Security and Privacy (SP)*; IEEE: New York, NY, USA, 2020; pp. 11–19.
33. Van Bavel, R.; Rodríguez-Priego, N. *Testing the Effect of the Cookie Banners on Behaviour*; JRC Technical Reports; Publications Office of the European Union: Luxembourg, 2017; pp. 7–20.
34. Akkus, I.E.; Weaver, N. The Case for a General and Interaction-Based Third-Party Cookie. *arXiv* **2015**, arXiv:1506.04107. Available online: https://arxiv.org/abs/1506.04107 (accessed on 17 January 2022).
35. Degeling, M.; Utz, C.; Lentzsch, C.; Hosseini, H.; Schaub, F.; Holz, T. We value your privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy. Network and Distributed System Security Symposium (NDSS). *Inform. Spektrum* **2019**, *4*, 1–11.
36. The General Data Protection Regulation (GDPR) and the ePrivacy Directive (ePR) Affect How You as a Website Owner May Use Cookies and Online Tracking of Visitors from the EU. Available online: https://www.cookiebot.com/en/gdpr-cookies/ (accessed on 23 December 2021).
37. The Ultimate Guide to Buying Privacy Management Software. Available online: https://www.cpomagazine.com/data-protection/the-ultimate-guide-to-buying-privacy-management-software (accessed on 14 February 2021).
38. Best Consent Management Platforms (CMPs) for Publishers. Available online: https://headerbidding.co/best-consent-management-platforms/ (accessed on 23 December 2021).
39. Karunaratne, T. For Learning Analytics to Be Sustainable under GDPR—Consequences and Way Forward. *Sustainability* **2021**, *13*, 11524. [CrossRef]
40. Šta je GDPR i Kako Će Uticati na Industriju 'Online' Oglašavanja? Available online: https://www.netokracija.rs/aleksandar-petkovic-gdpr-regulativa-137840 (accessed on 6 April 2022).
41. *OneTrust Privacy Management Software. OneTrust User Guide*; OneTrust: Atlanta, GA, USA, 2018.
42. Cookiebot. Available online: https://www.cookiebot.com/en/ (accessed on 7 April 2022).