KVKK KİŞİSEL VERİLERİ KORUMA KURUMU Kişisel Verileri Koruma Dergisi
www.kvkk.gov.tr Cilt:6 Sayı:2 Geliş:23.10.2024
Kabul:20.12.2024

Türkiye'de Kullanıcıların Bilgi/İzin Bildirimlerine İlişkin Algıları ve Tepkileri

Didem, GÜNGÖR FIRAT
Radyo Televizyon Üst Kurulu, Üst Kurul Uzmanı
didemgungor@rtuk.gov.tr
ORCID ID: 0009-0004-3017-3364

ÖZ

Avrupa Birliği'nin öncülük ettiği düzenlemeler, hizmet sağlayıcılara kullanıcıyı çerezler hakkında bilgilendirme ve kullanıcının açık rızasını alma sorumluluğunu yüklemektedir. Bu nedenle web siteleri, bilgi/rıza bildirimlerini kullanıcıları bilgilendirmek ve izin istemek için kullanırlar.

Bu çalışmanın birincil kaygısı, bilgi/rıza bildirimlerinin ve dolayısıyla yasaların kullanıcılar üzerindeki etkisini incelemektir. Mevcut çalışma, konuyla ilgili literatür ışığında şu soruları sormaktadır: Kullanıcıların bilgi/rıza formları hakkındaki bilgi ve algıları nelerdir, bu formlara nasıl tepki verirler ve rızalarını etkileyen faktörler nelerdir? Daha önceki çalışmalar daha çok AB bölgesi ve ABD'ye odaklanırken, bu çalışma Türkiye'ye odaklanır. Türkiye'deki kullanıcı davranışlarını anlamak için 56 katılımcı ile çevrimiçi bir anket yapılmıştır. Çalışma, bilgi/rıza bildirimlerinin, kullanıcıların gizlilikle ilgili kararlarında optimal karar vermeyi desteklemediği sonucuna varmıştır.

Anahtar Kelimeler: Çerezler, gizlilik, GDPR, KVKK, bilgi/rıza bildirimleri

User's Perception And Reactions To Informatıon/Consent Notices In Türkiye

ABSTRACT

The regulations led by the European Union impose the responsibility of informing the user about the cookies and obtaining the explicit consent of the user. For this reason, they use information/consent notices on their websites to inform users and ask for consent.

The primary concern of this study is to examine the effect of information/consent notices and, therefore, laws on users. The current study asks the following questions in the light of literature related to the subject: What are the users' knowledge and perceptions about the information/consent forms, how do they react to these forms, and what are the factors that affect their consent to these forms. While previous studies mostly focused on the EU region and the US, this study focuses on Türkiye. In order to understand user behaviour in Türkiye, an online survey was conducted with 56 participants. The study concluded that information/consent notices do not support optimal decision-making in users' privacy-related decisions.

Keywords: Cookies, privacy, GDPR, PDPL, information/consent notices (ICN)

Atıf Gösterme Güngör Fırat, D., (2024). Türkiye'de Kullanıcıların Bilgi/İzin Bildirimlerine İlişkin Algıları ve Tepkileri, *Kişisel Verileri Koruma Dergisi. 6*(2), 1-32.

1-INTRODUCTION

Privacy in the virtual world has become a hot topic for both practical applications and academic research, with the dramatic spread of internet users around the world. In recent years, it has enacted privacy laws all over the world to protect personal privacy against 'big data'. The European Union GDPR (General Data Protection Regulation) pioneered these legal regulations. Türkiye, which is in the European Union membership process, has put into effect the PDPL (Personal Data Protection Law) on April 7, 2016, based on the EU's pre-GDPR directive (95/38/EC). Arrangements are similar to each other in terms of the rules they set and their goal is basically to inform and support the user so that they can take rational steps in their decisions regarding their data. Under the transparency principle, service providers must obtain user consent to collect and use personal data. Websites commonly use cookies to collect information and regulations require service providers to supply 'clear and understandable' information about cookies to users. Thus, 'informed and freely given' consent can be obtained from the user. In this context, it can be questioned whether the law obligations literately authorise the user and help protect their online privacy.

Many studies in the past mention that the measures to protect personal data are ineffective and insufficient. While most studies reveal the prevalence of misunderstanding and lack of knowledge about the mechanisms that inform and enable users to make rational decisions (Kulyk et al., 2021; McDonald & Cranor, 2010), some other studies argue that online tracking is inevitable regardless of user awareness.(Abrardi et al., 2021; Sanchez-Rola et al., 2019; Utz et al., 2019) However, user information and consent forms produced by exploiting the vulnerabilities of the law easily direct the user to give consent through methods such as highlighting and nudging. (Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019) Besides, factors such as self-efficiency, specific features of the website, risk perception can also be effective in disclosing personal data. (Boerman et al., 2018; Kulyk et al., 2018; Milne et al., 2009)

It is crucial to state that different studies have given different names to the pop-ups appearing to inform or obtain consent from users: Consent management platforms (Nouwens et al., 2020), consent notices(Utz et al., 2019), cookie consent notices(Abrardi et al., 2021), cookie disclaimer(Kulyk et al., 2018, 2021). After examining the pop-ups encountered on the most frequently visited websites, it was seen that some designs used were only informative, while others had both informative and user consent functions. For this reason, this study calls these pop-ups 'Information/Consent Notices' (ICN).

This study assesses the effectiveness of legal measures by investigating the impact on users of information and consent forms, which are required by law and are frequently encountered while browsing the net. Above all, the study focuses on Türkiye. There are almost no studies on the effectiveness of the Personal Data Protection Law (PDPL), although it has been 5 years since the implementation. To test PDPL's ability to put website users in a better position in terms of online privacy, it poses the following research questions:

1-What is the user's knowledge and perception about the ICNs (Information/Consent Notices)?

2-How do users react to the ICNs?

3-What factors are effective in user's decisions about the ICNs?

To find the answers to these questions, I conducted an online survey with 56 participants. The survey was evaluated using both quantitative and qualitative methods. It was concluded that ICNs, the legal method for protecting personal data, fall far short of the goal of ensuring privacy. Participants are disturbed by the forms they encounter constantly, as well as they avoid interacting with them, ignore them, or react indiscriminately. They are also quite reluctant to get information provided by the forms. Although users see these forms frequently, they have inadequate and misleading information about their function and purpose. After all, factors such as the service genre provided by the website, the dependability of the website, the content of the messages may all play a role in deciding to disclose individual data.

2-BACKGROUND and LITERATURE REVİEW

Technical Background

Cookies

Web browser programmer Lou Montulli coined the term "cookie" and Netscape Communications use cookies in 1994 to ensure reliable use of the shopping site.(Montulli, 2000) "Cookies are small data structures sent from a Web server to your browser and saved on your hard drive in a text file. They are nothing more than a string of characters (letters and numbers) that store certain pieces of information about you." (Peters & Sikorski, 1997 p.1486)

The operation of cookies is not complicated. During website visits, various personal information of users is saved on the user's computer through browsers such as Google Chrome Microsoft Edge. The web server recalls these identifying information stored on the user's computer during the same website visit. Thus, information is not requested repeatedly for each visit. (Castelluccia & Narayanan, 2012) Web servers can remember the user's movements and information during past visits, thanks to the cookies. They are also used to determine the advertising target audiences of the companies and to generate accurate post traffic besides the main purpose of providing stateful navigation.

Using cookies provides many advantages and disadvantages. When a user visits a website for the first time, visual elements such as photos and pictures, as well as website preferences such as language, are stored in the computer memory. When the user returns to the same website, existing records save time by allowing them to skip filling out forms. (Peng & Cisna, 2000) It also offers an "individualised" market for website owners.(Lyon, 2006) It seems to be helpful for the server but at the same time, it is a source of concern for the user. While cookies improve the user's browsing experience, they also increase the privacy problem. What makes cookies dangerous in terms of privacy is not the information stored on users' computers, but how and for what purpose the personal information made accessible through cookies will be used by various institutions and organisations. (Edenberg & Jones, 2020 p.89-90)

Types of cookies can lead to different consequences in terms of online privacy. We can classify cookies according to their source as first-party and third-party cookies.(Castelluccia & Narayanan, 2012 p.3; Skouma & Léonard, 2015 p.41) First-party cookies are created by the website the user visits. They establish a direct relationship between the web server and the user. (OneTrust, 2020) They can be controlled, and their function is more specific. On the other hand, web servers can also allow cookies created by third parties for their websites. Banner advertisements on some web pages are displayed through third-party cookies. The user's web page browsing history is tracked, and the most relevant advertising content is presented to the user. Third-party cookies introduce new parties into the relationship between the user and the web provider, making it more complex and difficult to manage. (Article 29 Data Protection Working Party, 2013; Skouma & Léonard, 2015)

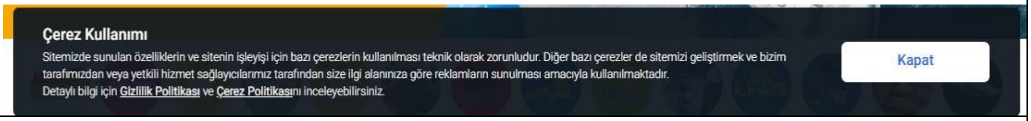
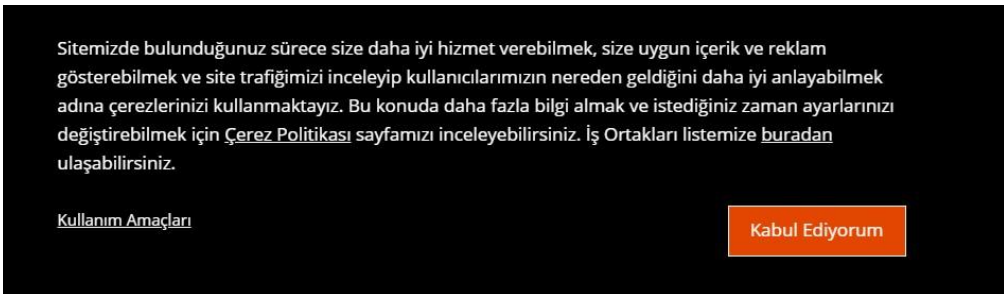
Another classification according to their storage time is "temporary cookies" (session cookies) and "persistent cookies" (Kulyk et al., 2018). Temporary cookies store user information only while the website is open and are automatically deleted while the website is closed. Short-term recordings, such as the products in the shopping cart, pose less risk to user privacy. (Kulyk et al., 2018) On the other hand, persistent cookies are not deleted even if the web browser is closed; the user needs to go to extra lengths to remove them. Long-term repositories can be used to access the user's preferences, interests, identity information, and friends. (Borgesius et al., 2015; ICO, 2021) They can be used for behavioural targeting or personal advertising. According to W3Techs, 23.1 per cent of all websites use persistent cookies, including well-known names like Google, YouTube, Facebook, Yahoo and cookies are used by 41.9% of all websites.(W3Techs,2021)

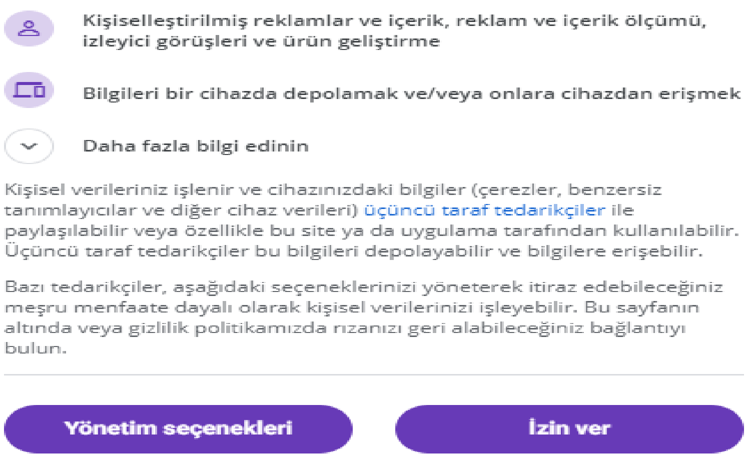
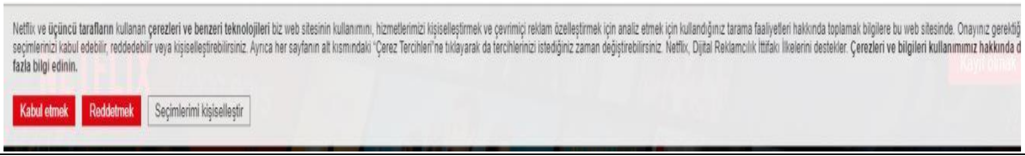
Grouping ICNs

Websites, as required by law, add ICNs to the screen to provide information about the cookies and to obtain permission to use them. Although the laws specify the features that consent notices must include, they do not identify a uniform design. Thus, websites already have a broad range of ICN designs. To determine the most commonly used ICN designs in Türkiye, I examined the pop-ups that provide information about cookies and ask for explicit consent. I visited the top 50 most visited websites in Türkiye according to Alexa.com rating, one by one and took the screenshots of the pop-ups.(Alexa, 2021) Then, I have classified them based on the options they presented to the user. *Table 1* shows the classified groups, definitions, and examples.

Table 1

Groups of information/consent notices (ICNs) from Türkiye's 50 most popular websites (according to Alexa.com rating)

Groups	Definitions-Examples
Only information	These pop-ups inform the website uses various cookies and provides a link with detailed information about cookies. It does not include an option to request consent. It has only a cross in the top corner to close the pop-up or just the close button. 14 of the 50 websites use this design. For example, 'Hepsiburada.com' has such a design:  Çerez Kullanımı Sitemizde sunulan özelliklerin ve sitenin işleyişi için bazı çerezlerin kullanılması teknik olarak zorunludur. Diğer bazı çerezler de sitemizi geliştirmek ve bizim tarafımızdan veya yetkili hizmet sağlayıcılarımız tarafından size ilgi alanınıza göre reklamların sunulması amacıyla kullanılmaktadır. Detaylı bilgi için Gizlilik Politikası ve Çerez Politikasını inceleyebilirsiniz.
Single-option	These pop-ups inform the website that uses various cookies and provides a link with detailed information about cookies. It provides a single option- 'accept'. 4 of the 50 websites use this design. For example, 'trthaber.com' has such a design:  Sitemizde bulunduğunuz sürece size daha iyi hizmet verebilmek, size uygun içerik ve reklam gösterebilmek ve site trafiğimizi inceleyip kullanıcılarımızın nereden geldiğini daha iyi anlayabilmek adına çerezlerinizi kullanmaktayız. Bu konuda daha fazla bilgi almak ve istediğiniz zaman ayarlarınızı değiştirebilmek için Çerez Politikası sayfamızı inceleyebilirsiniz. İş Ortakları listemize buradan ulaşabilirsiniz.
Two-option	These pop-ups inform the website uses various cookies and generally provides a link with detailed information about cookies. It provides a double option- 'accept' and 'manage'. 25 of the 50 websites use this design. For example, 'google.com' has such a design:

	 Kişiselleştirilmiş reklamlar ve içerik, reklam ve içerik ölçümü, izleyici görüşleri ve ürün geliştirme Bilgileri bir cihazda depolamak ve/veya onlara cihazdan erişmek Daha fazla bilgi edinin Kişisel verileriniz işlenir ve cihazınızdaki bilgiler (çerezler, benzersiz tanımlayıcılar ve diğer cihaz verileri) üçüncü taraf tedarikçiler ile paylaşılabilir veya özellikle bu site ya da uygulama tarafından kullanılabilir. Üçüncü taraf tedarikçiler bu bilgileri depolayabilir ve bilgilere erişebilir. Bazı tedarikçiler, aşağıdaki seçeneklerinizi yöneterek itiraz edebileceğiniz meşru menfaate dayalı olarak kişisel verilerinizi işleyebilir. Bu sayfanın altında veya gizlilik politikamızda rızanızı geri alabileceğiniz bağlantıyı bulun.
Three-option	These pop-ups inform the website uses various cookies and generally provides a link with detailed information about cookies. It provides a triple-option- 'accept', 'reject' and 'manage'. 3 of the 50 websites use this design. For example, 'netflix.com' has such a design:  Netflix ve **üçüncü tarafların** kullanan **çerezleri ve benzeri teknolojileri** biz web sitesinin kullanımını, hizmetlerimizi kişiselleştirmek ve çevrimiçi reklam özelleştirmek için analiz etmek için kullandığınız tarama faaliyetleri hakkında toplamak bilgilere bu web sitesinde. Onayınız gerektiğ seçimlerinizi kabul edebilir, reddedebilir veya kişiselleştirebilirsiniz. Ayrıca her sayfanın alt kısmındaki "Çerez Tercihleri"ne tıklayarak da tercihlerinizi istediğiniz zaman değiştirebilirsiniz. Netflix, Dijital Reklamcılık İttifakı İlkelerini destekler. **Çerezleri ve bilgileri kullanımımız hakkında d fazla bilgi edinin.**

Why Does the Usage of Cookies Require User Consent?

Cookies collect, store, and facilitate the reuse of personal data from internet users. Given this functionality, obtaining explicit consent from individuals whose data is stored and used is critical for safeguarding their privacy and security. Cookies can collect a variety of data, including demographic information and browsing patterns, which can subsequently be used to improve user experience, give tailored content, and target advertising. However, there are serious questions about how and by whom this information may be used when such personal data is stored and used. Unauthorized sharing or misuse of data collected through cookies poses risksto user privacy and could result in potential security breaches. Cookies also make it possible totrack users' preferences and surfing histories, which enables the development of comprehensiveuser profiles. These profiles can be used for sensitive purposes like financial forecasting or behavioural analysis, in addition to targeted advertising. (Jayakumar, 2021) Consequently, usersmay experience a vulnerability in privacy, as organizations or companies amass extensive knowledge about individuals' online behaviors without their explicit consent. This emphasises how crucial consent is to guaranteeing that information gathered via cookies is handled sensiblyand in accordance with the law and ethical norms. This situation has led to the necessity of protecting users' data privacy rights (Edenberg & Jones, 2020)

Without strong privacy protections, people are exposed to data misuse, which can lead to discrimination, identity theft, and other negative outcomes. As a result, there is growing agreement among academics and policymakers that legal frameworks need to change in order to guarantee users' rights to data privacy in a world that is becoming more linked. (Edenberg &Jones, 2020)

The European Union (EU) and other countries implemented laws like the GDPR (General DataProtection Regulation) and KVKK (Personal Data Protection Law) to ensure that individuals' personal data is collected, processed, and stored in a transparent and secure manner. These ruleswere created to safeguard users' right to privacy, stop data abuse, and make sure businesses getusers' express consent before collecting or using their data. In an increasingly interconnected digital world, the regulations seek to address growing concerns about identity theft, data breaches, spying, and the misuse of personal information.

Legal Background

Türkiye has made various regulations for protecting personal data as a requirement of becoming a member of the European Union. The EU has regulations on protecting online privacy, which keep very wide geography within its sphere of influence, including Türkiye. This study includes EU legislation as well because Turkish laws are based on EU laws and fall within the scope of them. Parts of laws regarding cookies will be explained in the context of the scope of this work.

The EU Regulations

There are two basic regulations of the EU regarding cookies. The first is GDPR (General Data Protection Regulation), which replaces Directive 95/46/EC, and the second is Directive 2009/136/EC, also known as the "Cookie Law" (Meyers, 2018; Trevisan et al., 2019), which is complementary to GDPR.

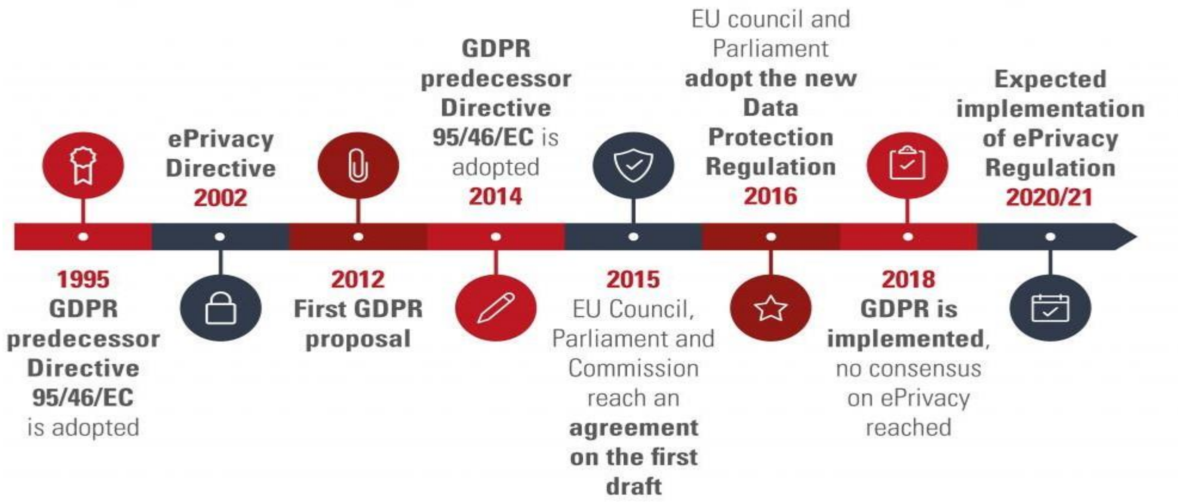

1995 GDPR predecessor Directive 95/46/EC is adopted
ePrivacy Directive 2002
2012 First GDPR proposal
GDPR predecessor Directive 95/46/EC is adopted 2014
2015 EU Council, Parliament and Commission reach an agreement on the first draft
EU council and Parliament adopt the new Data Protection Regulation 2016
2018 GDPR is implemented, no consensus on ePrivacy reached
Expected implementation of ePrivacy Regulation 2020/21

Figure 1: The History of general data protection regulations Source:(European Data Protection Supervisor, n.d.)

GDPR (General Data Protection Regulation)

The European Commission aimed to enhance control over one's data, raise awareness, ensure informed and free consent while creating the GDPR.(Strycharz et al., 2020).Responsibility for the consequences of online behaviour has been left to the user who is aware of rights and has a high level of knowledge. (Human et al., 2020; Strycharz et al., 2020) It has been claimed that it bypasses the bureaucracy and creates an effect similar to the Copernican Revolution. (The Copernican Revolution refers to the concept of the "cognitive powers of the individual".)(Kuner, 2012) According to Kuner, GDPR is based on individual empowerment. The obligation of web pages to obtain "consent" from the user to process personal data increases users' awareness of online privacy and gives them active tasks.

Directive 95/46/EC, the EU's first legal regulation on protecting personal data, was published on 24 October 1995 and remained in force until GDPR (2016). The European Union Commission published a recommendation for comprehensive changes in the Directive on January 25, 2012, due to the increasing importance of protecting personal data with technological developments and the differences in current regulations (Albrecht, 2016), the GDPR draft was accepted by the EU Parliament in 2014 and came into force on 25 May 2018. (European Commission, 2018)GDPR is fully binding for all member states and will apply the rules uniformly.

GDPR has a broad range of implementation. It applies to all web page owners who wish to process the data of the population staying in EU countries. "Regardless of whether the processing takes place in the Union or not", the data operator or organization is within the scope of GDPR. (GDPR Article 3) For example, a real or legal person residing in Türkiye must comply with both GDPR and legal regulations in Türkiye if they use the data of individuals residing in EU countries.

GDPR defines various concepts in Article 4. First, it defines 'personal data' as "any information relating to an identified or identifiable natural person." (Article 4/1) Recital 30 acknowledges that website cookies make a person identifiable.(Recital No:30) Although cookies are the most common tracking method, the Directive on data protection also covers other techniques that store and access information available on a web user's terminal device. (Recital No:24-25, Giakoumopoulos et al., 2018)

Another important definition is "consent". GDPR's consent definition is more focused on user intent and is more elaborate than Directive 95/46/EC's. According to Article 4/11, the characteristics of "consent" are as follows: freely given, specific, informed and unambiguous indication of the data subject's wishes by a statement or by a clear affirmative action.

Furthermore, user consent is required for the websites to process personal data following the law. Article 6/1 expresses this requirement: "The data subject has given consent to the processing of his or her personal data for one or more specific purposes." There are also various exceptions, such as the fulfilment of a task in the public interest or the protection of the vital interests of the data subject. (Article 6/1)

Websites that will process personal data should follow a set of rules when requesting user consent according to GDPR. ‘The request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language’ (Article 7/2):

According to Article 29 Working Group, the information to be delivered to the user should be on the first page when the user first logs into the site in a clear, comprehensive and visible way. Users should have access to information about all cookies used for different purposes. It is also expected to inform about the storage period of cookies and how preferences for cookies can be changed. (Article 29 Data Protection Working Party, 2013)

E-Privacy Directive

E-Privacy Directive particulates and supplements the GDPR. (Article 1/2). E-Privacy Directive (2002/58/EC) contains legal regulations regarding cookies since 2002. It was amended in 2009 (Directive 2009/136/EC) and came into force in 2011.(European Data Protection Supervisor, n.d.)

The E-Privacy Directive, as amended in 2009, established user consent as a general rule based on clear and comprehensive information. Article 5/3 of the Directive explains this rule: "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information..."

According to the Directive, user consent must be freely given, taken on a specific subject and based on knowledge. In addition, the user consent must be given explicitly and together with the active behaviour of the users before the data processing activity starts. (Article 29 Data Protection Working Party, 2013) GDPR, which came into force later, adopted this rule and provided a more detailed explanation.

Turkish Personal Data Protection Law No:6698 (PDPL)

Turkish Personal Data Protection Law no. 6698 (PDPL), which came into force on April 7, 2016, determines the processing conditions of personal data and the data processors' responsibilities. This law was drafted largely under the guidance of Directive 95/38/EC. (Murat & Dülger, 2019) PDPL applies to 'natural persons whose personal data are processed' and 'natural or legal persons who process such data wholly or partially by automatic means or otherwise than by automatic means.' (Article 2)

PDPL, in parallel with the European Union legal regulations, sets the rule that "explicit consent" must be obtained to process the data. "Explicit consent" must have the following characteristics: freely given, specific and informed. (Article 3)

The law stipulates a general rule: "Personal data shall not be processed without obtaining the explicit consent of the data subject", but there are several exceptions, just like GDPR. (Article 5/1) (For detailed info: KVKP, 2018) PDPL holds data processors fully responsible for informing users. Data controllers must provide the identity of the data controller, the purposes for which personal data will be processed, the persons to whom processed personal data might be transferred, the method and legal cause of data collection and rights of the data subject. (Article 10)

According to Article 5/1, it is mandatory to fulfil the obligation to inform in an easy-to-understand, clear and plain language in all cases where personal data is processed.(PDPO, 2019)

Literature Review

Studies that put the user at the center of research related to online privacy appear to address the following issues: The first group explores users' perception and knowledge of cookies and other online tracking tools. (Ha et al., 2006; Kulyk et al., 2018, 2021; McDonald & Cranor, 2010; Miyazaki, 2008; Ur et al., 2012) The second group tries to understand how users respond to consent pop-ups while online browsing(Choi et al., 2018; Norberg et al., 2007; Schermer et al., 2014) and explores essential factors in users' behavioral reactions (leaving the website, trying to learn more. etc.) to cookies texts and online tracking. (Abrardi et al., 2021; Boerman et al., 2018; Degeling et al., 2019; Kulyk et al., 2018, 2021; Leon et al., 2013; Machuletz & Böhme, 2020; Milne et al., 2009; Nouwens et al., 2020; Sanchez-Rola et al., 2019; Utz et al., 2019)

Knowledge and Perceptions

Studies on web users' knowledge and perceptions about cookies and informative texts paint a clear picture illustrates users' lack of knowledge and misunderstanding. Early research such as Ha et al. (2006), McDonald et al. (2010), and Ur et al. (2012) show that there is a widespread lack of information and misunderstandings about informational texts regarding personal data. (Ha et al., 2006; McDonald & Cranor, 2010; Ur et al., 2012) Ha et al. divided 16 participants into 4 groups in a study conducted in Canada according to age and technical information criteria: younger/technical, younger/nontechnical, older/ technical, and older/non-technical. Focus groups were asked about their information and perceptions about cookies. It revealed that all focus groups lack knowledge about the useful and threatening aspects of cookies and are quite confused about their functions. Many participants thought cookies could carry viruses. In particular, the non-technical groups had a hard time understanding the working methods of cookies. The older/technical group had a relatively high knowledge of what information would be stored with cookies or what they were used for, but they had little idea about how to deal with them. (Ha et al., 2006) McDonald and Cranor supported the Ha et al.' results. They measured the knowledge and perceptions of American internet users about online advertising techniques by conducting a semi-structured interview and subsequent survey with larger participation. One-third of the respondents answered the question 'what is a cookie' as they were not entirely sure. While more thana third of respondents provided partially correct answers, only three said cookies can be used to serve ads based on users' interests. (McDonald & Cranor, 2010) What is surprising in the research is that internet users do not know how to protect their privacy, despite their intense concern about their data. (Kulyk et al., 2018, 2021; McDonald & Cranor, 2010) Ur et al. investigated users' attitudes and understandings about online advertising like McDonald&Cranor's study. They interviewed in 2011 with48 participants in the USA. The results showed the participants saw personalized advertising tools as athreat to their privacy. Behind this understanding, there was the idea that advertisers collect informationsuch as name, e-mail, and financial status that would lead to recognising the person. However, the participants misunderstood the tools that inform the user about the ads personalisation and thought thatthey could use their scanner and virus protection programs to deal with them.(Ur et al., 2012) There appears to be a mismatch between the information users require and the information they have about online privacy. Informative texts on websites that provide useful information about protecting personaldata frequently make the website appear less trustworthy (Kulyk et al., 2021) or be misunderstood. (Kulyk et al., 2021; Ur et al., 2012) Also, Miyazaki et al. discovered that disclosing the use of cookies alleviated privacy concerns in their studies investigating the effects of the website's use of cookies on users in the USA. According to the results, users' privacy concerns increase when cookies are used privately and the cookie usage explanation is welcomed by the user. Also, prolonged internet use reduced anxiety about cookies. (Miyazaki, 2008)

While awareness of online privacy was minimal between 2006 and 2012, when the relevant studies were conducted, it has also been limited in recent years, despite scandals such as Cambridge Analytica and frequent media discussions. Kulyk et al. surveyed 150 participants in 2017 in Germany before GDPR and revealed that some participants had never heard of the term "cookies." The majority lacked sufficient knowledge to comprehend how cookie disclaimers protect online privacy. Besides, some thought the cookies could be spyware or a sign showing that the website is not reliable. (Kulyk et al., 2018) They repeated the same study in 2018 after the GDPR came into force. Even after intense public debate about online privacy, users' knowledge about cookies (disclaimer) has not increased. (Kulyk et al., 2021) Furthermore, both the original and follow-up studies concluded that instead of seeing cookies as a useful tool, users found them to be highly offensive and undesirable while surfing. The surprising result of the follow-up study was that users were more accustomed to seeing cookies after legal regulations. (Kulyk et al., 2021) The obligations brought by the GDPR have not changed in favor of protecting personal privacy.

While the above studies focus on Canada, the EU area and mostly the US, rare studies conducted in Türkiye on protecting online personal data show users do not know what to do to protect online privacy. (Eroğlu, 2018; Taskaya&Talay, 2019) In 2018, Eroğlu conducted an online survey targeting university students who have a high interaction with the digital environment. Students are very concerned about the use of their data in the digital environment. Roughly half of the students use privacy settings to protect their privacy. However, the other half do not know what the privacy settings are for and how to use them. Students rarely read the information texts provided by websites, and only one-third are aware of the personal data protection law. (Eroğlu, 2018) From a different perspective, Taskaya and Talay have in-depth interviews with experienced employees working as experts in data protection. Experts (data audit specialist, IT Law specialist) say that there is a lack of information on protecting personal data in Türkiye and legal regulations regarding online privacy are mostly unknown to the user. (Taskaya & Talay, 2019)

Reactions and Factors

Studies of varying scope have provided insights into how users react to the consent notices they encounter during their online interactions, and by which factors these reactions are affected.

The concepts of privacy paradox and privacy fatigue appear to be important in understanding how users react to ICNs. The "privacy paradox" refers to the fact that web users tend to disclose personal information despite having serious concerns about their online privacy.(Norberg et al., 2007) As technologies that enable the collection, distribution, storage, and use of data strengthen, legislators and users' concerns about online privacy grow. However, users easily share their data with the websites. (Norberg et al., 2007) Choi et al. explain the privacy paradox with privacy fatigue. "Privacy fatigue" is based on the belief that individuals cannot effectively protect privacy in the virtual environment, and this belief can undermine privacy efforts.(Acquisti et al., 2017) Choi's study reveals that users' intention to share their data is heavily affected by online privacy fatigue. When people are tired, they tend to make fewer efforts to protect their data. Users develop an avoidant coping strategy by doing nothing. "Consent Fatigue", on the other hand, as a sub-tab of privacy fatigue, leads to unconscious choices, such as not reading informational messages about how personal data will be processed and used, giving consent quickly or quickly rejecting it (Schermer et al., 2014). The user may develop behaviours in which he does not consider the consequences to get rid of this interruption.

Research on whether consent notifications empower users in their decisions regarding online privacy generally paint a pessimistic picture. Some of them argue that digital tracking mostly continues despite the consent notifications therefore consent notices are "ineffective elements" (Abrardi et al., 2021; Degeling et al., 2019; Sanchez-Rola et al., 2019), while others argue that consent notices can use designs that can easily guide the user to give consent.(Kulyk et al., 2018, 2021; Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019) Sanchez-Rola et al. tested whether users could avoid online tracking if they wish by denying permission notices for the most popular 2000 European and Non-European websites for each time they visit. According to findings, 92% of websites already follow users through various technical methods before expressing consent notification. Only 4% offer a clear opt-out option with cookie notifications, and only 2.5% delete cookies. (Sanchez-Rola et al., 2019) The overwhelming majority of websites continue tracking even if users never allow cookies, and their responses to cookies are ineffective in protecting online privacy. (Sanchez-Rola et al., 2019) To support this research, Degeling et al. state that the existing technical mechanisms for personal data protection are insufficient after analysing 6579 websites in 28 member states of the EU. Websites store and use personal data with many other methods besides cookies such as third-party cookies, beacons, JavaScript. As a result, obtaining explicit consent is difficult. Besides, controlling third-party cookies is only possible with the cooperation of third parties. (Degeling et al., 2019) Abrardi et al. made mathematical modelling and measured the costs of users' preferences on consent notices. The banners informing users about cookie policies have too many options and require a long time to browse, cause users to give consent easily. The unwillingness to waste time "now" results in using personal data by platforms in the "future". Thus, consent notices cannot protect personal privacy due to time inconsistency. (Abrardi et al., 2021) These approaches illustrate that the user's awareness/consciousness is not essential although they manage properly privacy setting in the most optimal way.

However, other studies show that the consent notices are ineffective, as various methods can readily guide the user. The design of the consent notifications is quite effective at 'bypassing' users. (Kulyk et al., 2021; Machuletz & Böhme, 2020; Nouwens et al., 2020; Sanchez-Rola et al., 2019; Utz et al., 2019) Utz et al. studied the interactions of 82,890 users with consent notices over four months. The results show that the bars at the top and bottom of the screen received less interaction (2.9%: 9.6%, respectively). On the contrary, the ones in the bottom left corner were found to attract the most attention (33,1%). More users choose "accept all" in consent forms that offer two options: "accept all" and "reject all". Also, the content of the information given about cookies has almost no effect on user decisions. (Utz et al., 2019) The highlighted buttons and few option buttons increased the 'accept all' selection as well as the position of the consent notices on the web page. (Machuletz & Böhme, 2020; Utz et al., 2019) On the other hand, Nouwens et al. found that consent to share personal data increases by 22-23 percent if there is no reject button. As the number of options offered to the user increases, the approval rate decreases by 8-20%.(Nouwens et al., 2020) Likewise, the majority of consent notices use designs that are difficult to reject. While 50.1 per cent do not have the 'reject' option at all, only 12.6% have a 'reject' option that can be clicked with the same amount of effort as the 'accept' option. Buttons that provide detailed information about cookies are not clicked by 93.1%. (Nouwens et al., 2020) In addition, while the highlighted "accept all" button was preferred by 50.8% in smartphones, this rate remained at the level of 39.2% for the unhighlighted "accept all" one. (Utz et al., 2019) Studies show that the number of options, highlighting and nudging used in consent notifications are very effective in user behaviour. Pop-up designs that guide users are referred to as 'dark patterns.' (Nouwens et al., 2020) In dark pattern designs, "user value is supplanted in favour of shareholder value."(C. M. Gray et al., 2018 p.1) Websites hide options to protect personal data or use complex information forms that are not user-friendly with 'convincing' (Fogg, 2009) or 'nudging' designs (Acquisti et al., 2017). They negatively affect the autonomy of the user and the cleanliness of the decision-making process. Nouwens et al. revealed that "dark patterns" are quite common after analysing the 12,000 most widely used websites in the UK. Only 11.8% of the forms requesting user consent have features that comply with EU legal regulations. Utz et al.'s study examining consent notice designs from 1000 random websites confirms the prevalence of dark patterns. According to this study, 57.4% of the websites have designs that encourage the user to share their data.

Moreover, some other factors are also influential in the users' reactions to consent notices, such as self-efficacy (Milne et al., 2009), the type of information, the scope of data and period of data retention (Leon et al., 2013), risk perception(Boerman et al., 2018), the type of service offered by the website, thesite's reliability and frequency of use (Kulyk et al., 2021). According to Kulyk et al., users accepted thecookie disclaimer when they were familiar with the websites and were less concerned about their privacy. (Kulyk et al., 2021) It is seen that the risk perception mentioned by Boernman et al. is primarilyhigh in newly encountered websites. (Boerman et al., 2018) Milne et al. surveyed 449 participants in theUS and investigated how effective online self-efficacy (people's knowledge and ability to manage onlinethreats) is in protecting their privacy. They found that individuals with high self-efficacy are more likelyto engage in active behaviours to protect their privacy and avoid activities that they would define as risky. (Milne et al., 2009) Leon et al. examined different dimensions of users' tendencies to share their data with an online survey consisting of 2912 participants. The results suggest that the scope of the useand period of data retention have a wide impact on users' wishes for sharing data. While users do not want to disclose their browsing or location information on a social media account such as Facebook, they are more inclined to share their personal history and educational status. How long personal data will be used is another factor in user decisions. People are very reluctant to share data for more than a week. While almost no one wants to share sensitive information such as credit card number, phone number, instant location, nearly half of the participants tend to share less sensitive data such as browser version, gender or residence. (Leon et al., 2013) Besides, the online sphere becomes more reliable as the level of knowledge and skill increase in how websites protect visitors' data. (Milne et al., 2009) Kulyk et al., in their study before GDPR, found that some features of websites are effective as well as the content and design of information texts in user reactions. Users refrained from leaving websites that provide online banking and e-mail services, which are inevitable to use for business and daily life activities, even if they use cookies. But they also wanted to abandon the same websites hosting sensitive data. In addition, the website realibility has alleviated concerns about the cookies. The likelihood of opt-out is reduced for frequently used or well-known websites. Parallelly, the post GDPR follow-up study found that the features of the websites were still influential in abandonment behaviours. (Kulyk et al 2021) Boerman et al., on the other hand, investigates the effect of the perceived risk level and the belief that they can protect themselves with personal efforts on the behaviour of protecting privacy. Evaluating the results of a large-scale online survey conducted in the Netherlands, they reveal users perceive sharing their data as a threat at a very high rate. The higher the risk people perceive to their privacy, the more they strive for online security. Self-efficacy significantly increases protective behavior, while lack of technical knowledge on how to protect personal data hinders action. (Boerman et al., 2018)

3-METHODOLOGY

Research Questions

This study investigates the effectiveness of the laws regarding the protection of personal data in Türkiye. When the relevant literature is examined, it is discovered that most previous studies have been conducted in the United States and the European Union. Although the relevant law in Türkiye went into effect in 2016, no research has been found, except for a few studies on how PDPL measures are perceived by users, how much they are known, and what behaviours users exhibit to protect their online privacy. This study examines whether Türkiye's laws are an effective method of protecting personal data to fill the gap in the literature.

It also places the user at the centre because the laws delegate the authority to the user in decisions regarding online privacy. (European Commission, 2018; Kuner, 2012) However, It is thought that the ICN forms aiming to manage privacy settings do not empower the user for various reasons. Many past studies mention the prevalence of incomplete or incorrect information about protecting users' online privacy.(Ha et al., 2006; Kulyk et al., 2018, 2021; McDonald & Cranor, 2010; Ur et al., 2018) while some claim that users do not make an effort to protect online privacy. (Acquisti et al., 2017; Kulyk et al., 2018, 2021)Furthermore, dark patterns may undermine users' optimal decision-making abilities (Machuletz & Böhme, 2020; Nouwens et al., 2020; Utz et al., 2019) and users' reactions to ICNs are affected by various factors such as self-efficiency (Milne et al., 2009), features of shared data(Leon et al., 2013), website features (Kulyk et al. 2018) and risk perception. (Boerman et al., 2018)

In the light of previous studies, this study poses the following sub-questions specific to the Turkish region:

1. What is the user's knowledge and perception about ICNs offered by the websites?
2. How do users react to the ICNs they encounter while online surfing?
3. What are the factors affecting the reactions of the users to the ICNs?

Sampling

This study uses convenience sampling. It is a non-random sampling method in which the researcher collects data from his/her immediate surroundings. The primary advantage is that the data can be obtained easily, quickly and economically.(Brewis, 2014; Sedgwick, 2013) Besides, samples are convenient to use in both qualitative and quantitative research. Even so, the fact that the sample units are drawn from the researcher's circle calls the ability to represent the main mass questionably. Some argue that the data obtained by this method will only represent a subset of the population and will not be suitable for generalisation to yield meaningful results. (Fricker & Schonlau, 2016; Sedgwick, 2013)

Table 2 depicts the demographic distribution of the survey. 56 people answered the online survey. 55.4% of the respondents are female and 44.6% are male. Participants are between the ages of 18-55, but the majority (91%) are 26-45 years old. Every participant has a bachelor's or master's degree. 80.4% stated that they had no experience in information technology as a worker, student, employer, etc., whereas 19.4% are experienced and have worked for an average of 8.5 years.

Table 2

The demographic composition of the participants

		f	%
Gender	Female	31	54,4
	Male	25	44,6
Age	18-25	3	5,4
	26-35	19	33,9
	36-45	32	57,1
	46-55	2	3,6
Education	Bachelor	24	42,9
	Master	32	57,1
IT Experience	Yes	11	19,6
	No	45	80,4
	Total	56	100,0

Data Collection and Survey Design

The data were collected through a questionnaire developed for a similar study by Kulyk et al., whose validity and reliability tests were performed. In response to the research questions of this study, changes were made to the previously used survey in consultation with experts in the field. Since the survey aims to learn the feelings and thoughts of the people, it consists of many free-text questions. Unlike the original version of the questionnaire, some questions have been made multiple-choice to make them easy to answer. The survey was conducted in Turkish and online. It comprises five parts:

In *The General Part*, the most commonly used ICN form in Türkiye is shown and asked what its content and purpose might be. They were also asked to describe their feelings and reactions when confronted with such a form.

The ICN Specific Part contains the most commonly used ICN designs in Türkiye, as determined at the start of the study. The design, which provides both 'reject all' and 'accept all' options, has been added to four different designs for comparison although not included in the most frequently used designs. Thus, the questionnaire was divided into five groups, with random participants assigned to each group.

Participants were asked about their feelings, thoughts and reactions to each design. In addition, the possibility of clicking on links that provide extra information about cookies in ICNs was also asked. Finally, it was inquired as to how one reacts to pop-ups that must be interacted with to gain access to the website.

In *The ICN Ranking Part*, participants were shown all four different designs and asked to rank them from most to least likely to lead them to consent to the use of cookies.

In *The New ICN Part*, six fresh additions (A1-A6) were made to the standard cookie message, and it was asked whether these new versions would be preferred (to give consent) compared to the standard message.

The Demography Part asks age, gender, profession and IT experience of the participants.

Analysis Methods

This study uses both quantitative and qualitative methods in the analysis of the data. Answers to open-ended questions about knowledge, perception, and reactions to ICNs were discussed within the thematic analysis. All responses were coded and evaluated to understand the overall theme observed for the research question. Quotes from participant responses were used to support the themes.

Measurement was also used in the analysis. Measurement is the transformation of researched objects and events into numbers, symbols, and figures within the framework of certain principles. (P. S. Gray, 2007)

4-RESULTS

In this section, the findings of the survey are presented as headings related to each research question.

User knowledge and perception about ICNs

Knowledge

The following question was asked to the participants to assess their knowledge of ICNs:

The General Part (Q4)	'What could be the reason for this form to appear on the screen?

Common themes in responses are data collection, advertising activities, data security, and legal obligation.

Data collection: A significant portion of the participants (22.4%) said that these forms that appear on the screen aim to collect and use personal data. While the term 'collection' of personal data was most frequently used in the responses, the terms 'accessing' and 'storing' data were less frequently used: *'Collecting and using the data I use on the site (e-mail, telephone, etc.)'*

Advertising Activities: 18 respondents (36.7%) stated that websites collect information about users' interests, tastes, search histories, and then offer interesting advertisements to the user based on this information: *'Collecting some personal data from my search history and using it in advertising strategies.'* Some participants highlighted the beneficial aspects of advertising activities for them. *'Learning my behavior according to my needs and facilitating the provision of services to me.'* However, some respondents emphasised that personalised advertisements favour websites: *'My private information is collected and sold to others for advertising.'*

Data Security: According to some participants, these forms were seen as a way to inform them about data protection and to ensure data security during their online activities*: 'Informing, having control over the sharing of personal information..'*

Legal Obligation: 7 of the respondents said that these forms appear on the screen as a legal obligation. *'In order not to act against PDPL.'* The participants who provided this response did not explain why there is such a legal obligation or comment on the purpose of the law.

Perception

The following questions were given to participants to understand their perceptions of ICNs:

The General Part (Q5)	What were your thoughts and feelings when you encountered this message?
The ICN Spesific Part (Q8) (For one of the disclaimers G1-G5)	What were your thoughts and feelings while reading the consent form above?
The ICN Spesific Part (Q12)	Do the information in the forms (about what cookies do) affect your consent to cookies? Please explain your reasoning.

The themes encountered frequently in the responses were disturbance, apathy, distrust, misinformation/misunderstanding and pleasure.

Disturbance: Most of the participants stated that pop-ups on the screen disturb them. The main reason users dislike these forms is that they see them as an obstacle to reach the website: *'It is irritating to be subject to this requirement for site use.'* Another disturbing factor was that they needed extra time and effort to read, understand, approve or reject the forms: *'I see it as a waste of time.'*

Apathy: Many participants stated they do not care and read ICNs and ignore forms because they encounter them too frequently: '*At first I found it disturbing and challenging... but my initial reactivity is no longer there, I just walk by without looking.'* The fact that the participants were aware that these warnings were required by law caused them to disregard them. *'I ignored it because it was routine and procedural messages.'*

Distrust: Although the ICNs are thought to be user-friendly, a significant group said that when they saw the forms on the screen, they had negative feelings about their privacy and the reliability of the website. Using cookies by websites is perceived as a source of insecurity in itself: *'I think what is written there does not reflect the truth.'*

Misinformation and misunderstandings: The common point in the answers was confusion about what the ICNs do, the reason for being seen on the screen, or what consequences it might have on their privacy. Many participants think they cannot access the websites unless they consent to the use of cookies: *'If I don't agree, I think I can't handle my work on the site.'* Another missing information is that the users do not know clearly what the ICNs will have to protect their data. Besides, some users misunderstood the ICNs and said that it could be related to viruses on the website.

Pleasure: A few participants expressed satisfaction with this application, which informs them about the use of personal data and requests permission for using their data: *'I found it transparent and honest.'*

Moreover, cross-tabulation analysis was performed on the responses of those with and without IT experience to the question of whether they care about ICNs to see if knowledge influences perceptions about ICNs. According to the analysis, 72.7% with IT experience said they don't care about the information forms (that they were ineffective in their decision-making), while 51.1% with no IT experience said the same. According to this result, knowing about ICNs did not lead to perceiving ICNs as more important.

Table 3

Cross-tabulation analysis was performed to determine whether IT experience and non-IT experience take into account ICNs.

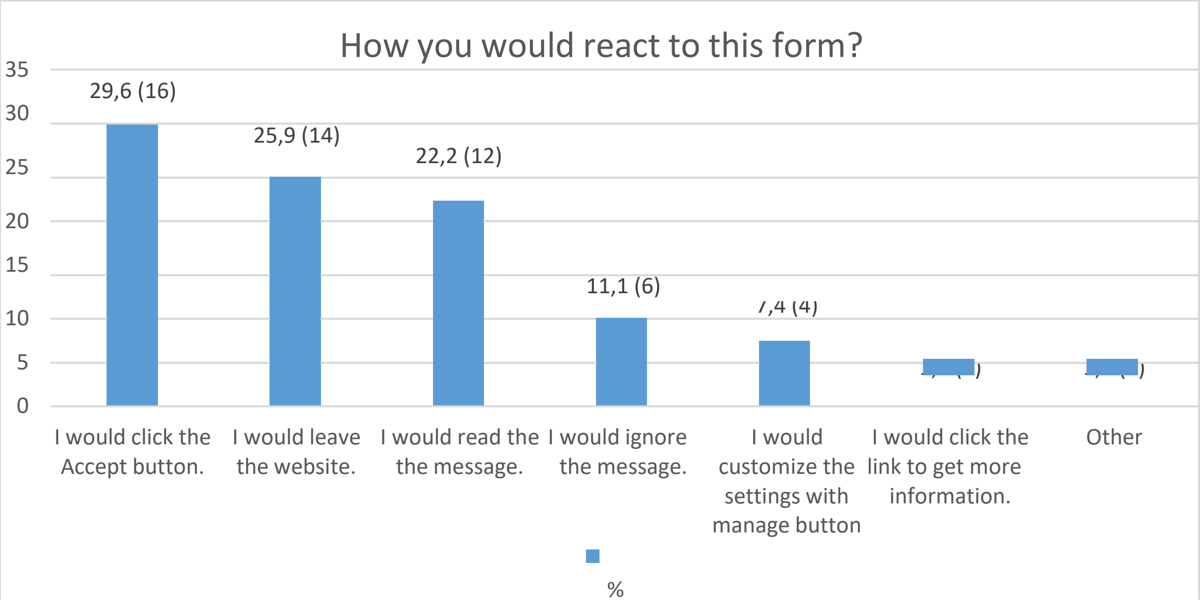
Do you have any experience in information technology (IT) as a student, employee, employer, etc?	Q12: Do the information in the forms (about what cookies do) affect your consent to cookies?		
	Yes	No	I don’t know
Yes	27,3%	72,7%	0%
No	33,3%	51,1%	15,6%

User reactions to the ICNs

The responses to the following questions were analyzed to comprehend how participants responded to the ICNs.

The General Part (Q6)	How you would react to this form?
The ICN Spesific Part (Q9)	How do you usually react to this form?
The ICN Spesific Part (Q10)	What do you think will happen as a result of your reaction to this form?
The ICN Spesific Part (Q11)	How do you usually react when you see a consent form that needs to be answered to access the website?
The ICN Spesific Part (Q13)	How likely are you to click on the "more information" link?

Graph 1 depicts the responses to the Q6. As seen in the graph, only 31.5% prefer options that require extra effort, such as managing settings (7.4%), reading the message (22.2%), or clicking the link for more information (1.9%). However, the most common response (29.6%) is to press the accept button. The second-highest rate (25.9%) is to stop visiting the website.



Graph 1: Answers to Q6

Table 4 depicts the survey groups as well as the design elements that were presented to the participants. Participants were divided into five groups, and each group was given a design and asked how they would react to it.

Table 4

Different ICN Designs shown participants in the five Groups

Group	ICN design
G1	**Only information:** These pop-ups inform the website uses various cookies. Using cookies does not include an option to request consent.
G2	**Single-option:** These pop-ups inform the website uses various cookies and it provides a single option- 'accept'.
G3	**Two-option:** These pop-ups inform the website uses various cookies and it provides a double option- 'accept' and 'manage'.
G4	**Two-option:** These pop-ups inform the website uses various cookies and it provides a double option- 'accept' and 'reject'.
G5	**Three-option:** These pop-ups inform the website uses various cookies and it provides a triple-option- 'accept', 'reject' and 'manage'.

Table 5 shows the responses to Q9 of participants assigned to each of the G1-G5 groups. To investigate the differences between the ICNs, the chi-square test was used to compare the answers in groups G1-G5. The test found no statistically significant differences between the groups ($\chi2$ = 7,161, p = 0,128 > p

= 0,05), indicating that all the ICNs in the study had a similar effect on the participants' decision to give consent.

Table 5

Chi-Square analysis investigating the difference in consent response between groups (G1-G5)

Groups	Q9: **How do you usually react to this form?**		Total	X^2	Sd	p
	'I would accept'	Responses other than 'I would accept'				
G1	6	14	20	7,161	4	0,128
G2	6	6	12			
G3	4	20	24			
G4	3	14	17			
G5	2	14	16			

The responses to Q9 and Q10 were also analysed using open coding, and they were basically as follows: accept, ignore, reject, and opt-out.

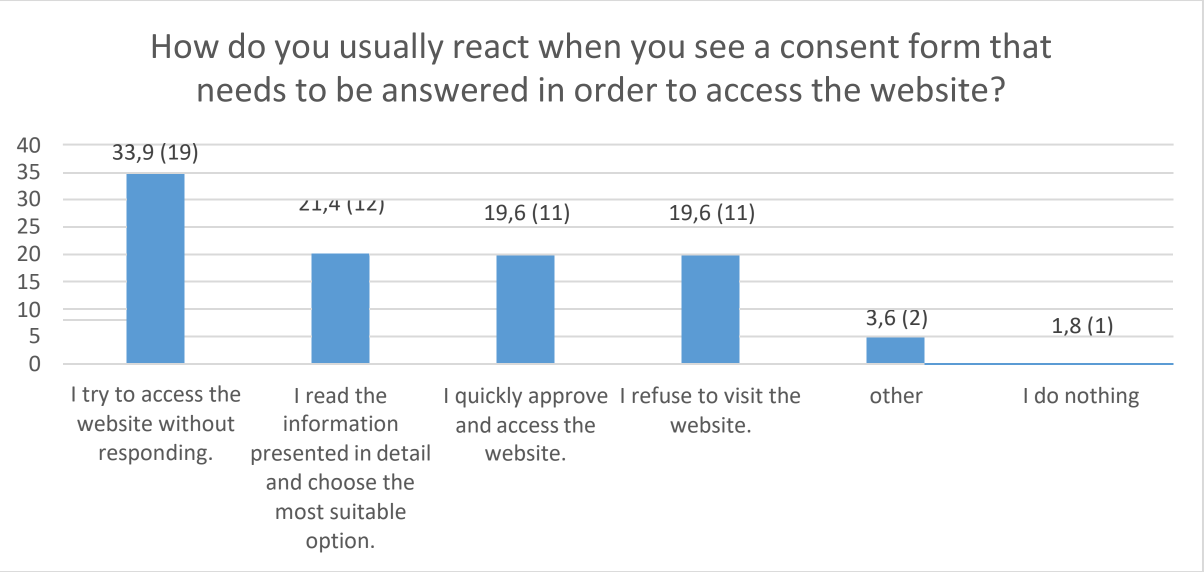
Accept: The majority of participants (35,7%) said they responded by giving consent to these forms. Most of the participants are aware that they are sharing personal data by accepting the forms and they think they will be exposed to more advertisements. *'I thought that my personal data would be recorded and I would be encouraged to do more online shopping in the future.'* Besides, another common belief is that once the forms are approved, they will use the website or use it more effectively.

Ignore: 23,2% said that they would continue their online activities without interacting with pop-ups. Participants expect to be greeted with the same warnings again on their next visit, after ignoring: *'If I ignore it, the same happens when I log back in, I ignore it again.'* They think it will have a neutral result for their privacy: *'I don't think it's a loss or a benefit for me.'*

Reject: 19,2% said that they refused ICNs to protect their online privacy. Participants choose the reject button when they want to keep control of their data or when they want to feel more secure. *'If I give permission, I think I am out of control and that I cannot claim rights for my data later.'*

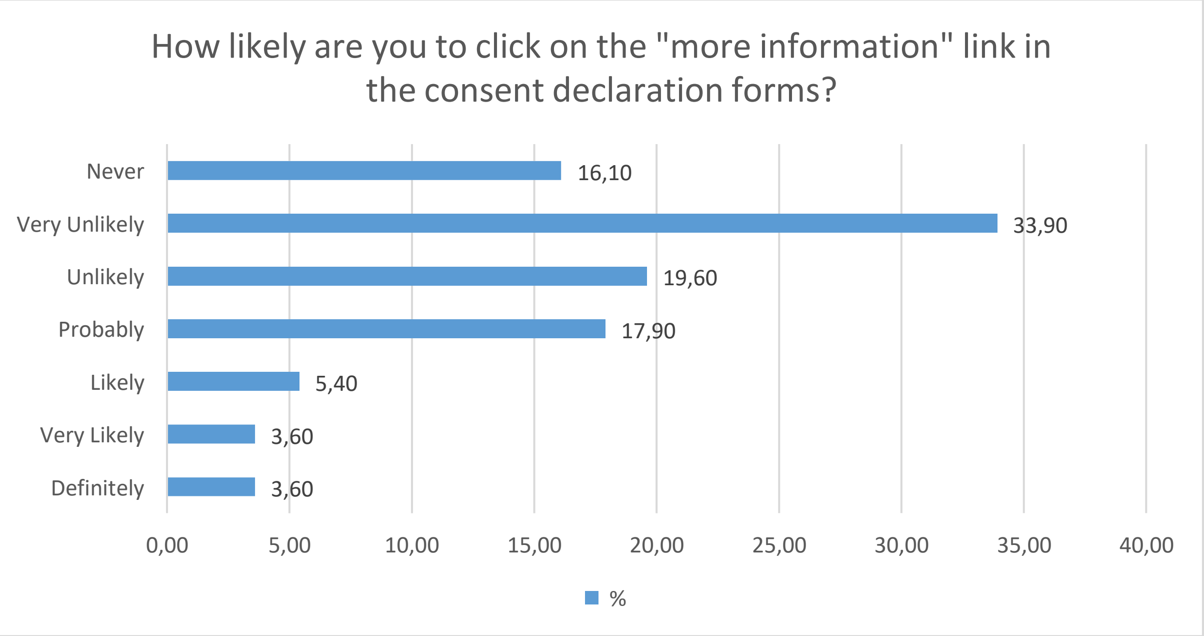
Opt-out: 17,8% stated that they stopped visiting the site when they encountered the ICNs. Participants thought that this method would prevent digital tracking. *'It can't follow me because I'm not on the site.'*

Graph 2 is listing how participants answered Q11. In cases where it is necessary to interact with pop-ups to reach the website, only 21.4% of respondents said they would carefully read the information presented to them and choose the best option; interestingly more (33.9% plus 1.8%) said they would search for ways to use the website without providing any answers. 19.6% stated they would quickly approve the ICNs in order to use the site and continue on their way.



Graph 2: Answers to Q11

Graph 3 shows the answers to Q13. According to responses, only 3.6% will definitely click on the link, while 16.1% will never click it. Furthermore, a sizable proportion of participants (69.6%) will not click on the information link.



Graph 3: Answers to Q13

A Kruskal-Wallis test was used to compare ICNs in groups G1-G5 in terms of the likelihood of clicking more information links. According to the result, there is a statistically significant difference between the G1-G5 groups. (p = 0,013 < p=0,05).

Table 6

Kruskal Wallis analysis investigating the difference between groups (G1-G5)

	Groups	N	Mean Rank	Sd	p
How likely are you to click on the "more information" link in the forms?	G1	20	42,43	4	0,013
	G2	12	56,63		
	G3	24	55,38		
	G4	17	36,79		
	G5	16	32,66		

Mann Whitney U analysis was performed for pairwise comparisons between groups to determine which group caused this difference. According to the test, the significant groups are; G1, G2, G3, G4, and G5. The reason for the differentiation is that people in the G2 and G3 are less likely to click on the link.

Table 7

Mann Whitney U analysis for pairwise comparisons in groups (G1-G5)

Groups	Pairwise comparisons	N	Mean Rank	p
G1	G2	12	20,46	**0,040**
	G3	24	25,79	0,052
	G4	17	17,35	0,374
	G5	16	15,56	0,121
G2	G3	24	18,92	0,721
	G4	17	12,12	**0,024**
	G5	16	11,19	**0,011**
G3	G4	17	16,41	**0,034**
	G5	16	15,38	**0,021**
G4	G5	16	16,03	0,563

Factors affecting the user's consent

The answers to the following questions were analysed to determine what factors influence users' consent to share their data:

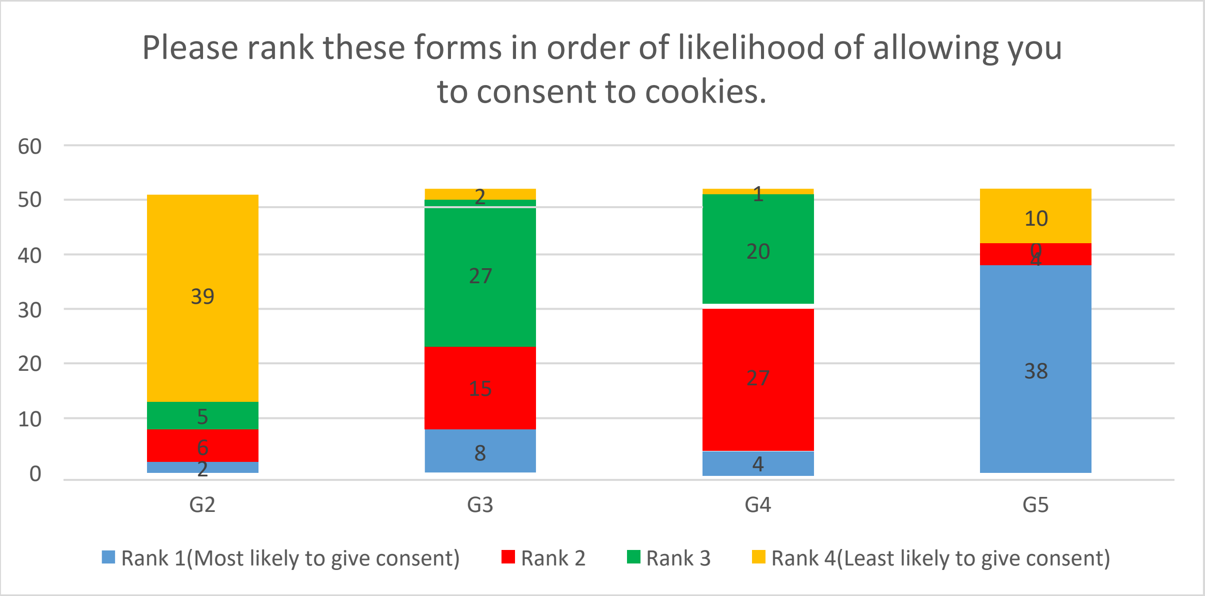
The ICN Spesific Part (Q12)	Does the information in the consent forms affect your consent to the cookies?
The ICN Spesific Part (Q14)	Which situations can convince you to consent to the cookies?
The ICN Spesific Part (Q15)	Which situations cannot convince you to consent to cookies?
The ICN Ranking Part (Q16)	Please rank these forms in order of likelihood of allowing you to consent to cookies.
The New ICN Part (Q18)	How would the following additions change the probability of giving consent to the forms?

After analysing the responses, the following topics have been identified that may affect the user's consent: The ICN design, text content, and features of the website.

The ICN design

Respondents were asked to rank the ICN designs shown in *Table 4* from most convincing to least convincing to consent. (The design in the G1 group is excluded because it has no option to consent.)

Graph 4 summarises the user responses. The most convincing design for sharing personal data is presented in the G5. 38 respondents (73%) stated that they are most likely to share their data when 3 options appear. Despite the notable difference, the second most preferred design for consent (15.3%) is the G3. This is followed by G4 and G2, respectively. Users frequently stated that providing more options increased their confidence. *'The amount of information and options offered gives me more confidence.'* In addition, 75% of respondents ranked G2 as the least likely to consent. Users stated that they dislike the G2 because it provides the fewest options (in parallel with the fact that they prefer the G5, which offers the most options). Presenting only one option causes the user to feel compelled and insecure to accept it: *'If the reject or the manage option are not provided, I think it's done as an order', 'I just think the accept button is not safe.'*



Graph 4: Numbers of participants who placed a pop-up design from the corresponding group (G2-G5) in each rank.

Text contents

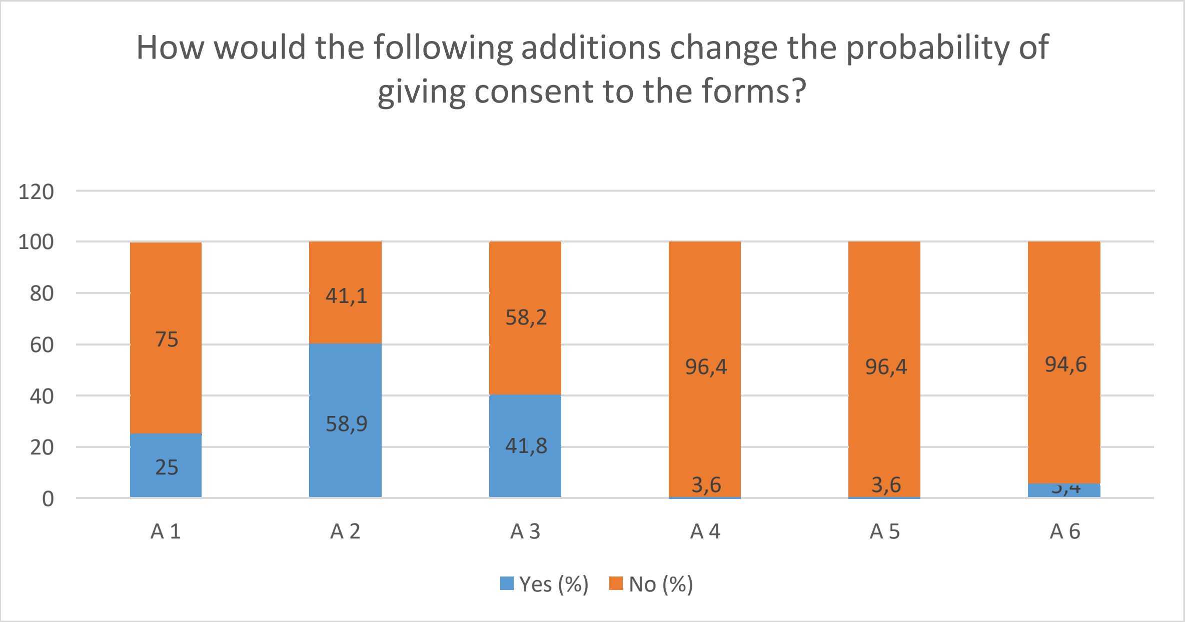
In order to understand the effect of the texts in the ICNs on sharing personal data, the standard message content was first shown to the 56 participants. They were then asked whether the message containing each addition (A1-A6) convinced them to consent compared to the standard message. *Table 8* present the standard messages and additions.

Graph 5 shows the responses to whether they preferred the new message texts that resulted from each addition to the standard message. Participants answered 'yes' when they preferred the new version and 'no' when they preferred the standard message. The findings indicate that the text contents of ICNs are effective in displaying user consent. The Cochran Q test was used to compare across all participants to see if some additions were more likely to cause participants to consent, and it revealed significant differences.(p = 0,000 < p = 0,05) The reason for the differentiation is due to the high number of positive reactions to the A2. Participants mostly prefer A2 (58.9%), followed by A3 (41.8%) and A1 (25%). However, the additions that received the most negative reaction were A4 and A5 (96.4%), followed closely by A6 (94.6%).

Table 8

Standard messages and additions presented to the participants

Standard message	"This site uses cookies. Cookies are used to improve our service to you."
Adition 1 (A1)	We also use cookies to show you personalized ads.
Adition 2 (A2)	We also use cookies to increase user security.
Adition 3 (A3)	We also use cookies to improve your user experience and provide you with the necessary information.
Adition 4 (A4)	We also use cookies to collect data about you.
Adition 5 (A5)	We also use cookies to collect data about you and sell this data at high prices.
Adition 6 (A6)	We also use cookies to sell our advertising space on the website more expensive since the data is very valuable today.



Graph 5: Numbers of participants who considered a corresponding new ICN (A1-A6) either more or less likely to lead them to consent for using cookies.

The participants were also asked the reason for their preference. The themes that emerged from the participants' responses were benefits, distrust and advertising.

Benefits: When the user advantage is emphasised in the message content (A1, A2, A3), more participants prefer new versions. It was found more reassuring that the websites stated they would act in favour of the user. *'The user security statement gives me confidence on the site.'* Also, the benefits that may accure in favour of the service provider are frequently cited as a reason for not approving: *'I don't want him to take advantage of me.'*

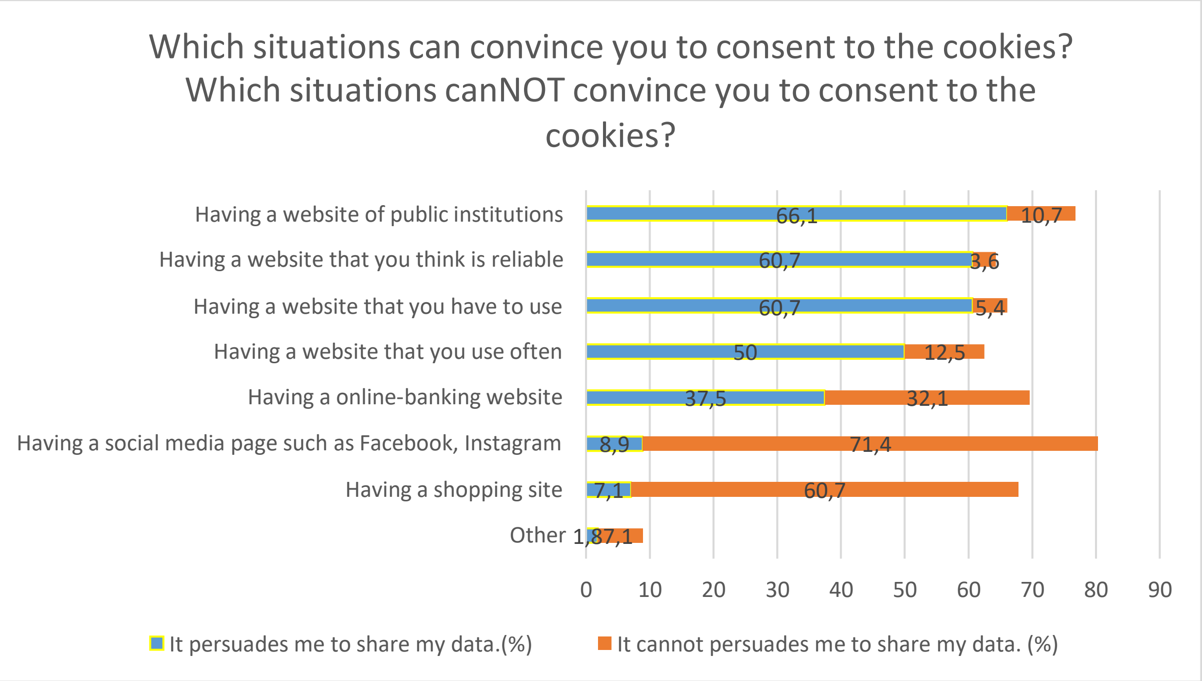
Distrust: The common theme for all additions (A1-A6) is that some users indicate they will not trust their service provider at all. *'Using my information is unreliable under all circumstances.'* Particularly, the participants think that the texts in A1, A2 and A3 have the purpose of directing them. *'Perception is created in my interest'*

Advertising: Most users interpreted the phrase 'improving the user experience' in A3 as more advertisements. *'I think ads will increase.'* In addition, they did not prefer the A1 version, where the expression 'personalised advertising' is present. (Yes 25%; No 75%) *'I don't want ads to target me specifically.'* Similarly, it was deemed offensive to indicate that personal data will be used for advertising purposes in versions A4, A5, and A6: *'The feeling of being marketed is not pleasant'*

Websites features

To understand whether the characteristics of the websites are effective in users' consent, they were asked which situations could and could not persuade them to consent to cookies.

As shown in the *Graph 6*, features such as the service provided by the website (public service, banking, shopping..), the website's reliability, familiarity with the website, and the website's importance can have both positive and negative effects on the user's desire to share their data.



Graph 6: Percentage of respondents' answers to whether they would be persuaded to share their data for each different website feature

Feature of the service: While 66.1% of the participants stated that they would persuade webpages that provide public services to share their data, 10.7% stated that public services websites could not convince them. While there is a high proclivity to consent for public service, the opposite is true for social networking and shopping sites. A sizable proportion (71.4%) are hesitant to share their data with social media platforms such as Facebook and Instagram. This figure is also quite high for shopping websites. (60.7%)

Reliability of the website: The responses clearly show that the tendency to disclose personal data with trusted websites is high (60.7%). Besides, 3.6% stated that they would not consent even if the website was reliable.

Familiarity with the website: 50% stated they would be persuaded to consent to the ICNs if they use the website frequently. In addition, 12.5% stated they would not want to give consent even if they were familiar with the site.

The importance of the website: Users are more inclined to give consent for the websites they have to use. While 60.7% of the participants stated they would approve ICNs on websites that are of high importance to them, 12.5% of users state that this situation cannot convince them to give consent.

5. DISCUSSION

The primary goal of laws such as GDPR and PDPL is to allow users to choose whether to share data, to determine which type of data to share, and to have various cookie information. The law assigns the user the duty to protect their data and provide an environment to make the optimal decision. For this, they require service providers to inform the user about cookies and to get their consent. However, the fundamental condition for achieving this goal is undoubtedly that the user knows what ICNs are for and how to manage them. The study's findings clearly demonstrated that even a group with a high level of education has confusion and a lack of knowledge about ICNs. In the participant answers, it was seen that users focused on only one function of the ICNs or misinterpreted. The 'data collection' and 'advertising activities' functions, which are frequently encountered in participant answers, are actually the purpose of using cookies. It has been reported by fewer users that ICNs are used to provide information and obtain consent. The functions of cookies and ICNs get mixed up.

Moreover, seeing these forms on the screen has created a negative perception for most users. The vast majority feel uncomfortable when they see ICNs, and it's almost common practice to get rid of them immediately. An interesting result from the participant answers is that seeing ICNs on the screen causes distrust of the website. Participants no longer care as they see ICNs too often. Lack of information, misunderstandings, distrust, indifference and discomfort seem to prevent users from spending time effectively reading and understanding them. Few users satisfy with these forms. In this context, ICNs are far from their target. To enable to use ICNs effectively, it's helpful to clear up the misunderstanding and lack of information. Changing the perception of 'constant annoying pop-ups' is vital for the user. The users should be reminded that they have the authority to manage privacy. The lack of a standard design of ICNs may be the reason for the differences in users' perceptions. To ensure transparency, a common ICN form for all websites can be created by legislators.

Survey respondents rarely read and care about the information contained in the ICNs and the links provided for more information. Users develop different behavioural patterns instead of reading the information presented and making the optimal decision. Most of the users prefer the accept option to get rid of ICNs as soon as possible. When asked in the General Part about their reaction to ICNs, 29.6% of respondents said they would click accept, while 11.1% said they would ignore ICN. Besides, in situations where interaction with ICNs was mandatory, the responses were no less of an attempt to get rid of the pop-up without informing. (The rate of those who say they agree quickly is 19.6%, the rate of those who say they try to reach the website without interacting with pop-ups is 33.9%) Some studies have stated that the reason for this is consent fatigue.(Nouwens et al., 2020) The survey results revealed that the user can no longer care about the ICNs encountered frequently. In addition, boredom, reluctance to read long texts and the desire to enter the website as soon as possible were seen to trigger consent fatigue. Also, a large number stated that they do not trust the information provided in any way and they believe they will be subjected to online monitoring under any circumstances. In addition, while only 3.6% would definitely click the links providing more information, 69.6% implied they would not click on this link. The answers to this specific question matched the answers given in the G1-G5 groups, where the reaction to each design was asked separately. The key point in user reactions is that the extra effort is often unpopular. In the responses, there is almost no response to customise the settings. Again, a substantial proportion (25.9%) state that they will leave the website to protect their online privacy, instead of opting to customise the settings or reject them. These rates do not show significant differences in the G1-G5 groups. (23.07%, 16.6%, 13.3%, 30%, 16.6%) The answers reveal that the user is reluctant to read more, get information, manage settings, etc. in alternative situations.

Service providers fulfil the measures required by law, and users are looking for ways to throw of these pop-ups in various ways. As a result, both parties carry out the process of informing and obtaining consent with a theatrical performance. By using dark patterns extensively, service providers can interfere with consent decisions. It casts a shadow on the 'freely given' decision stipulated by the law. The responses of the participants in the G1-G5 groups were closely related to what was presented to them. Where 'reject' is included in the pop-up options (G4-G5), respondents are more likely to choose rejection. (30%, 44.4%). According to the results, when the 'accept' and 'reject' options are presented atthe same time, the accept and reject reaction rates are the same. (30%) If only the 'accept' option is included, the rate of those who give consent increases to 66.6%.

The results of this study showed that the ICN design, text content, and website characteristics were effective in consenting behaviour. While ICNs with more meaningful options are preferred, users ranked the alternative with only the 'accept' option last. This was because they found more meaningful options to be more reliable. In addition, the user must understand why personal data is collected. Participants cared about their interests and were more approving of alternatives that seemed to benefit them. However, when the benefits of the service provider were emphasised, respondents mostly expressed disapproval. The A2 option was preferred because it emphasized the user benefit. Yet, previous research and these survey results indicate that the user does not prefer to read the content. The content of the texts will, of course, be effective in this case if the user is willing to read it. Also, website characteristics affect giving consent. The fact that a website belongs to public institutions or is thought to be reliable increases the tendency to consent. Users, on the other hand, are unwilling to share their personal information on shopping or social networking sites. In this case, increasing reliability means it can collect more data for a web page. Public service pages are less queried by the user. The indispensabilityof the service offered by the website increases the possibility of consent. The illusion that services cannotbe obtained without consent boosts consent for these web pages.

6. CONCLUSION and LIMITATION

Websites collect, use and store people's information to act more functionally on behalf of both the user and themselves. Cookies are the most common tools used to collect data. The collection of data through cookies facilitates the user's online experience. But it also brings with it heated debates about protecting personal private space. Many countries have attempted to ensure that personal data is secure in the virtual world. Laws require service providers to provide detailed information to users about data collection methods, reasons, and usage patterns, as well as obtain consent. The main goal of the transparency provided by the ICNs is to allow users to have a say over and manage their data.

This study investigates the users' knowledge, perception and reaction, as well as the factors affecting giving consent to the ICNs. The survey, which included 56 participants, provides an assessment of the effectiveness of mandatory practices brought by legal regulations. According to the findings, users do not appear to fully comprehend the function of these forms. Participants' information about ICNs is partially correct, blurry or contains misunderstandings. Besides, most participants find the ICNs annoying. Even if the users fully and clearly understand the functions of the forms, they are quite reluctant to read the texts, manage the settings and learn more to ensure their online privacy. They are prone to ignoring forms or responding to them without giving them much thought. It seems unrealistic to expect them to carefully read the ICNs and make an optimal decision, in the new world that is fascinated by speed, on all the pages visited during the day. Also, service providers can make directions that will enable the user to give consent, with different form designs prepared by adhering to the GDPR or PDPL rules. Dark patterns are so common that almost no website offers an explicit option for the user to refuse cookies. Legal obligations, which were fulfilled by superficial means, have turned into a boring, uncomfortable, incomprehensible format. As a result, problematic and obligatory consent arises.

The design elements of the forms, as well as the reliability of the website, the type of service it offers and the text content, all influence the participants' willingness to consent. Users are more likely to give consent for pages they trust, are familiar with, and must use. In addition, the emphasis on user benefit in text content facilitates user consent. Having website-specific factors enabled means that ICNs are met with different responses in different situations. Once again, the effectiveness of ICNs suffers, as providing detailed information is not the only effective reason for the consent.

There are a number of legal and useful ways to increase the efficacy of user consent under data privacy regulations such as the PDPL and GDPR. One key proposal is standardized consent mechanisms across websites. In order to make user interactions with privacy settings dependable and transparent, standardising consent methods entails developing consistent cookie consent notice (ICN) graphics and wording across websites. Governments could set regulations for how these ICNs should look, such as defining a standard layout, color scheme, and terminology, so users easily recognize and understand consent choices without confusion. For instance, each ICN may have uniform "Accept," "Reject," and "Customise Settings" buttons that are prominently displayed and labelled. While the content is simple and free of technical jargon, the graphic design might highlight user choices with contrasting colours. By setting these standards, users would experience predictable, transparent interactions with ICNs, making it easier to exercise control over data use. Mandatory Data Privacy Impact Assessment is another suggestion. Before processing personal data, service providers may conduct a mandatory data privacy impact assessment. By concentrating on potential security flaws in areas like data security, user consent, and data minimisation, it looks at how data is gathered, kept, and utilised. It may also necessitate an effect analysis and system restructuring. Web pages are subject to obligations when this structure is established.

In addition, the issue of stricter supervision of large technology companies such as Google and Meta, which use big data, should be brought to the agenda. Recently, there has been much discussion about how technology corporations exploit big data solely for commercial objectives and are not held accountable. Companies using big data can undergo stricter controls not only for legal compliance but also for how they handle users' data.

Enhanced user education and transparency are also crucial; governments should promote awareness campaigns about digital privacy rights and empower individuals to manage their data actively. Additionally, revising data minimization principles in laws could help companies only request data essential for the service, reducing excessive data collection.

Lastly, it is important that the determined legal rules and sanctions are dynamic to adapt to constantly changing technologies. The digital world is witnessing very important developments every day. There is a rapid transition from the environment where big data is discussed to the reliability of artificial intelligence. Personal data protection laws should be updated periodically, taking into account newly developing technologies and data processing methods in the digital environment. This is especially true in new areas of data processing such as artificial intelligence, big data, biometric data.

References

Abrardi, L., Cambini, C., & Hoernig, S. (2021). ``I don't care about cookies!" Platform Data Disclosure and Time-Inconsistent Users. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3806112

AcquistiAlessandro, AdjeridIdris, BalebakoRebecca, BrandimarteLaura, Faith, C., KomanduriSaranga, Giovanni, L., SadehNorman, SchaubFlorian, SleeperManya, WangYang, & WilsonShomir. (2017). Nudges for Privacy and Security. *ACM Computing Surveys (CSUR)*, *50*(3). https://doi.org/10.1145/3054926

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review (EDPL)*, *2*. https://heinonline.org/HOL/Page?handle=hein.journals/edpl2&id=313&div=&collection=

Alexa. (2021). *Alexa - Top Sites in Turke - Alexa*. https://www.alexa.com/topsites/countries/TR

ARTICLE 29 DATA PROTECTION WORKING PARTY. (2013). *ARTICLE 29 DATA PROTECTION WORKING PARTY Opinion 06/2013 on open data and public sector information ('PSI') reuse THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA*. http://ec.europa.eu/justice/data-protection/index_en.htm

Boerman, S. C., Kruikemeier, S., & Zuiderveen Borgesius, F. J. (2018). Exploring Motivations for Online Privacy Protection Behavior: Insights From Panel Data. *Communication Research*. https://doi.org/10.1177/0093650218800915

Borgesius, Z., Mcdonald, F. J. ;, Frederik, D., Zuiderveen Borgesius, J., & Mcdonald, A. M. (2015). *UvA-DARE (Digital Academic Repository) Do Not Track for Europe Do Not Track for Europe*. http://ssrn.com/abstract=2588086

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brewis, J. (2014). The Ethics of Researching Friends: On Convenience Sampling in Qualitative Management and Organization Studies. *British Journal of Management*, *25*(4), 849–862. https://doi.org/10.1111/1467-8551.12064

Burton, D. (2000a). *Research Training for Social Scientists : A Handbook for Postgraduate Researchers*. Sage Publication. https://ebookcentral.proquest.com/lib/lboro/detail.action?docID=483368

Burton, D. (2000b). *Research Training for Social Scientists: A Handbook for Postgraduate Researchers*. SAGE Publications.

Castelluccia, C., & Narayanan, A. (2012). Privacy considerations of online behavioural tracking. . *European Network and Information Security Agency (ENISA).*

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*.

Clarke, V., Braun, V., & Hayfield, N. (2015). *Qualitative Psychology: A Practical Guide to Research Methods* (J. A. Smith, Ed.). SAGE Publicaitons.

Comley, P. (2002). Online survey techniques: Current issues and future trends. *Interactive Marketing 2002 4:2*, *4*(2), 156–169. https://doi.org/10.1057/PALGRAVE.IM.4340174

Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., & Holz, T. (2019). *We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy*. https://doi.org/10.14722/ndss.2019.23378

Edenberg, E., & Jones, M. L. (2020). Troubleshooting AI and Consent. In *The Oxford Handbook of Ethics of AI*. The Oxford Handbook of Ethics of AI. https://philpapers.org/rec/EDETAA-2

Eroğlu, Ş. (2018). Dijital Yaşamda Mahremiyet (Gizlilik) Kavramı ve Kişisel Veriler: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Öğrencilerin Mahremiyet ve Kişisel Veri Algılarının Analizi. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi*, *35*(2), 35. https://doi.org/10.32600/huefd.439007

European Commission. (2018). *Progress on EU data protection reform now irreversible following European Parliament vote*. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_186

European Data Protection Supervisor. (n.d.). *The History of the General Data Protection Regulation | European Data Protection Supervisor*. Retrieved October 5, 2021, from https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

Fogg, B. (2009). A behavior model for persuasive design. *ACM International Conference Proceeding Series*, *350*. https://doi.org/10.1145/1541948.1541999

Fricker, R. D., & Schonlau, M. (2016). Advantages and Disadvantages of Internet Research Surveys: Evidence from the Literature: *Http://Dx.Doi.Org/10.1177/152582202237725*, *14*(4), 347–367. https://doi.org/10.1177/152582202237725

GDPR. (n.d.). *Recital 30 - Online Identifiers for Profiling and Identification - General Data Protection Regulation (GDPR)*. Retrieved October 5, 2021, from https://gdpr-info.eu/recitals/no-30/

Gerson, K., & Horowitz, R. (2002). *Observation and interviewing. Qualitative research in action*.

Giakoumopoulos, C., Buttarelli, G., & O'Flaherty, M. (2018). *Handbook on European data protection law - 2018 edition | European Union Agency for Fundamental Rights*. https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). *The Dark (Patterns) Side of UX Design*. https://doi.org/10.1145/3173574.3174108

Gray, P. S. (2007). *The Research Imagination : An Introduction to Qualitative and Quantitative Methods*. https://ebookcentral.proquest.com/lib/lboro/reader.action?docID=307439

Gurau, C. (2007). The Ethics of Online Surveys. In *https://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/978-1-59140-792-8.ch012*. IGI Global. https://doi.org/10.4018/978-1-59140-792-8.CH012

Ha, V., Inkpen, K., al Shaar, F., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. *Conference on Human Factors in Computing Systems - Proceedings*, 833–838. https://doi.org/10.1145/1125451.1125615

Human, S., Gsenger, R., & Neumann, G. (2020). *ePub WU Institutional Repository End-user Empowerment: An Interdisciplinary Perspective Conference or Workshop Item (Published) (Refereed) End-user Empowerment: An Interdisciplinary Perspective*.

Jayakumar, L. N. (2021). Cookies 'n' consent: An empirical study on the factors influencing website users' attitudes towards cookie consent in the EU. *DBS Business Review*, *4*, Article 72. https://doi.org/10.22375/dbr.v4i0.72

ICO. (2021). *Cookies and similar technologies*. Information Commsisioner's Office; ICO. https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/

Kulyk, O., Gerber, N., Hilt, A., & Volkamer, M. (2021). Has the GDPR hype affected users' reaction to cookie disclaimers? *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/CYBSEC/TYAA022

Kulyk, O., Hilt, A., Gerber, N., & Volkamer, M. (2018, July 1). *"This Website Uses Cookies": Users' Perceptions and Reactions to the Cookie Disclaimer*. https://doi.org/10.14722/eurousec.2018.23012

Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*. https://papers.ssrn.com/abstract=2162781.

KVKP. (2018). *Turkish Personal Data Protection Law no. 6698 • Kişisel Verilerin Korunması Mevzuatı • KVKP*. https://www.kisiselverilerinkorunmasi.org/kanunu-ingilizce-ceviri/

Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., & Cranor, L. F. (2013). What matters to users? Factors that affect users' willingness to share information with online advertisers. *SOUPS 2013 - Proceedings of the 9th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2501604.2501611

Lessig, L. (2009). *Code: And Other Laws of Cyberspace*.

Lyon, D. (2006). Theorizing Surveillance. In *Theorizing Surveillance*. Willan. https://doi.org/10.4324/9781843926818-5

Machuletz, D., & Böhme, R. (2020). Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(2), 481–498. https://doi.org/10.2478/popets-2020- 0037

May, T. (2011). *Social Research Issues, Methods and Process* (Forth Edition). Open University Press.

McDonald, A., & Cranor, L. F. (2010). Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising by Aleecia McDonald, Lorrie Faith Cranor :: SSRN. *PTRC 2010*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092

Meyers, W. A. (2018). C Is for Cookie: Is the EU's New Cookie Law Good Enough to Protect My Data. *International Lawyer*, *52*. https://heinonline.org/HOL/Page?handle=hein.journals/intlyr52&id=513&div=&collection=

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, *43*(3), 449–473. https://doi.org/10.1111/j.1745-6606.2009.01148.x

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy and Marketing*, *27*(1), 19–33. https://doi.org/10.1509/jppm.27.1.19

Montulli, L. (2000). HTTP State Management Mechanism. *Bell Laboratories, Lucent Technologies*. https://www.rfc-editor.org/rfc/rfc2965.txt

Murat, D., & Dülger, V. (2019). *AVRUPA BİRLİĔİ GENEL VERİ KORUMA TÜZÜĔÜ BAĔLAMINDA KİŞİSEL VERİLERİN KORUNMASI*. https://orcid.org/0000-0003-4034-5436

Norberg, P., Horne, D. R., & Horne, D. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*.

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April 21). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3313831.3376321

Oldendick, R. W. (2012). Survey Research Ethics. *Handbook of Survey Methodology for the Social Sciences*, 23–35. https://doi.org/10.1007/978-1-4614-3876-2_3

OneTrust. (2020). *Cookie Consent | Comply with Cookie Laws | Products | OneTrust*. https://www.onetrust.com/products/cookie-consent/

PDPO. (2019). *Communique on the Procedures and Principles to be Followed for the Fulfillment of the Obligation of Informing*. www.kvkk.gov.tr

Peng, W., & Cisna, J. (2000). HTTP cookies – a promising technology. *Online Information Review*, *24*(2), 150–153. https://doi.org/10.1108/14684520010330346

Peters, R., & Sikorski, R. (1997). SITE FINDER: Cookie Monster? *Science*, *278*(5342), 1486b–11487. https://doi.org/10.1126/SCIENCE.278.5342.1486B

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P. A., & Santos, I. (2019). Can i opt out yet? GDPR and the global illusion of cookie control. *AsiaCCS 2019 - Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security*, *12*, 340–351. https://doi.org/10.1145/3321705.3329806

Schermer, B. W., Custers, B., & van der Hof, S. (2014). The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. *Ethics and Information Technology*.

Schillewaert, N., Langerak, F., & Duhamei, T. (1998). Non-probability Sampling for WWW surveys: a comparison of methods'. *Journal of the Market Research Society*, *1*(40), 307–321.

Sedgwick, P. (2013). Convenience sampling. *BMJ*, *347*(oct25 2), f6304–f6304. https://doi.org/10.1136/BMJ.F6304

Sharp, M. K., Glonti, K., & Hren, D. (2020). Online survey about the STROBE statement highlighted diverging views about its content, purpose, and value. *Journal of Clinical Epidemiology*, *123*, 100–106. https://doi.org/10.1016/J.JCLINEPI.2020.03.025

Skouma, G., & Léonard, L. (2015). *On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection*. 35–60. https://doi.org/10.1007/978-94-017-9385-8_2

Strycharz, J., Ausloos, J., & Helberger, N. (2020). Data Protection or Data Frustration? Individual Perceptions and Attitudes towards the GDPR. *European Data Protection Law Review (EDPL)*, *6*. https://heinonline.org/HOL/Page?handle=hein.journals/edpl6&id=430&div=&collection=

TASKAYA, M., & TALAY, Ö. (2019). Dijital Gözetimin Pazarlama Amaçlı Aracıları: "Çerezler" ve Çerez Kullanımında "Açık Rıza." *Akdeniz Üniversitesi İletişim Fakültesi Dergisi*.

Trevisan, M., Traverso, S., Bassi, E., Mellia, M., di Torino, P., & Cyber Secu-, E. (2019). *4 Years of EU Cookie Law: Results and Lessons Learned*. 126–145. https://doi.org/10.2478/popets-2019-0023

Ur, B., Leon, P. G., Cranor, L. F., Shay, R., & Wang, Y. (2012). Smart, useful, scary, creepy: Perceptions of online behavioral advertising. *SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security*. https://doi.org/10.1145/2335356.2335362

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field ACM Reference Format. *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, 18. https://doi.org/10.1145/3319535.3354212

W3Techs. (2021). *Usage Statistics of Persistent Cookies for Websites, October 2021*. https://w3techs.com/technologies/details/ce-persistentcookies