

THE

Gökçe

Fine PRINT

January 2019

76

ARE COOKIES A THREAT FOR OUR PRIVACY?



ARE COOKIES A THREAT FOR OUR PRIVACY?

Internet users consider that their activities on the Internet are being monitored almost every day for different reasons. Sometimes, the ads of a product that we've looked for via search engine on the previous day show up the next day and we are surprised by the suggestions offered by the internet sites as if they know us better than us. Moreover, there are even those who claim that the issues spoken during any conversation are shown as advertisements on the Internet in some ways. However, we continue to use the Internet sites without paying attention to what is written in the small boxes that we face when we first enter them. These small boxes often contain details about how our information and activities are collected and used through cookies, so that we can make better use of the websites.

Although we got off to a bad start about cookies, it is undeniable that some cookies, as they say in the small boxes, are necessary to make better use of many websites. For example, the role of the cookies in the functioning of e-commerce sites, which we have been using too much in everyday life, is enormous. Suggestion of any products similar to the products you bought or looked at in previous purchases on an e-commerce site or remembering the products that you already added to the shopping cart even after the website is closed and then opened is possible by means of the cookies. In 1994, when a company called Netscape Communications was developing an e-commerce application, a computer programmer Lou Montulli was thinking of the great value to the e-commerce of remembering the information in the user's shopping cart and used cookies for the first time.

So what are these cookies?

Cookies are small text files with the .txt extension stored on the users' devices through the users' browsers, as opposed to a computer program that is actually believed. Contrary to what many people think, they cannot access other data stored on the hard disks of these devices when placed on a computer or mobile device.

Although the information gathered via different types of cookies and their use may vary, the operational logic of all cookies is the same. When a user logs in to a website for the first time, the internet server assigns a user-specific and distinctive identity. This identity is stored on the computer or mobile device on which the browser is run and in case the user enters the website again, the browser sends cookie to the server, allowing the website to remember the user. In fact, cookies function as a kind of memory of the internet running through protocols that provide data flow.



Why have cookies become a privacy issue?

First of all, it is useful to give an insight about the purposes and types of cookies to answer this question. Cookies may be used for a variety of purposes including the ability to continue with the information of the last page on a

website, to remember our login information such as the user name and password and preferences and to present content and ads in line with our interests and needs. Different types of cookies are used to achieve these purposes.

There are two types of cookies with regards to retention period: session cookies and persistent cookies. A session cookie is stored in temporary memory and is not retained after the browser is closed. As we will explain below, the type of cookie required to provide instantly expected benefit from the website is basically these session cookies. For example, the cookies that keep your information until the session is closed on the websites providing online banking services are session cookies. As to persistent cookies, they remain in the devices until they are deleted from the browser by users or until they expire.

Persistent cookies are used for provision of customized content and collection of statistical data about user's website activity.

The main types of cookies that create privacy concerns for users are third party cookies.

Although first-party cookies are cookies sent by the website you have entered, third-party cookies are cookies that are created and placed on your device by different internet subjects placed on the website you are visiting. Different advertisings we observe on websites are provided with these cookies; more specifically, ad servers track user behavioral information to serve customized advertising on another website. These third party cookies may be found on many web sites and accepted as the most undesirable types of cookies with the concern that it may cause privacy and security risks creating a behavioral profile based on our surfing history and the content we visited.

Is the data collected through cookies may be accepted as “personal data”?

Although there is no specific provision regarding the data processed by the cookies in the Law on the Protection of Personal Data (Law), this issue may be interpreted in the light of the European Union personal data legislation. It might be said that the data obtained by the cookies are considered as personal data to the extent that the relevant data allows to identify the natural person taking into account the General Data Protection Regulation (GDPR) and the Directive 2002/58/EC on privacy in electronic communications (e-Privacy Directive). While the e-Privacy Directive, which applies to any type of cookies whether it processes personal data or not, is always one of the main sources; GDPR also should be considered in case the cookies process personal data. Since there is no specific legislation subject to the cookies in Turkey, the important point is whether the relevant cookie is collecting personal data.

Therefore, companies or individuals who provide services through an online platform and use cookies and/or third-party interactions such as extension/button in this platform, should evaluate in detail the information gathered by the cookies used and should obtain the consent of the related persons if they use the cookies collecting personal data. Otherwise, relevant companies or individuals would be faced with allegations that no consent has been obtained for processing of personal data.



Answers. Not theories.

Gokce Attorney Partnership

Editors:



Assoc. Prof. Dr. Ali Paslı
ali.pasli@gokce.av.tr



Yağmur Yollu
yagmur.yollu@gokce.av.tr



Bahadır Bektaş
bahadir.bektas@gokce.av.tr



Ahmet Başaran
ahmet.basaran@gokce.av.tr



Dila Erol
dila.erol@gokce.av.tr



Fatih Ermiş
fatih.ermis@gokce.av.tr

About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, debt recovery, real property, and commercial litigation. Please visit our web site at www.gokce.av.tr for further information on our legal staff and expertise.

Please contact us at
contact@gokce.av.tr

0 212 352 88 33

The Fine Print is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to receive further information, please contact Gokce Attorney Partnership. No content provided in The Fine Print can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Fine Print was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.

For further information please contact us at contact@gokce.av.tr