

Modern Technologies Law



<http://doi.org/10.22133/mtlj.2025.467629.1352>

Cookies and the ability to invade privacy in cyberspace

Farangis Mansoori 

Assistant Prof., Department of Law and Social Sciences, Payame Noor University, Tehran, Iran.

Article Info	Abstract
Original Article	Today, protecting privacy in cyberspace is a major concern for the people of the world. The lack of a single organization that can manage the online space with its restrictive and strict rules has caused some websites to use small text files called cookies to collect data from users and use them for marketing in advertising networks and use third-party websites with the help of different technologies... Although it can be argued that this is a kind of marketing strategy and in most cases, it is not dangerous. However, this can lead to security concerns and privacy violations because most websites do not ask permission to use cookies and set them in the user's browser. The main question in this article is how and to what extent cookies can violate users' privacy. In response, we will say that although cookies play an essential role in enhancing the user experience and facilitating personalized interactions on the web in the broad digital technology landscape, they also come with risks that users should be aware of them. In general, there are two main risks; the first risk is a violation of users' privacy and the second risk is a security vulnerability.
Received: 12-06-2024	
Accepted: 07-08-2024	
Keywords: Cookie Privacy Security Personal information Cyberspace	
*Corresponding author e-mail: f.mansoori@pnu.ac.ir	
How to Cite: Mansoori, F. (2025). Cookies and the ability to invade privacy in cyberspace. <i>Modern Technologies Law</i> , 6(11), 377-395.	
Published by University of Science and Culture https://www.usc.ac.ir Online ISSN: 2783-3836	

1. Introduction

In cyberspace, privacy is the most important concern. Everyone who is online likes to keep their privacy safe. One of the things that can violate this privacy is internet cookies, which are designed to exchange information between the user's browser and the website. Cookies contain all kinds of information needed to navigate the desired website. For this reason, they are very important for e-commerce companies and advertising agencies. Almost in most web browsing, we are given a notification that "This website uses cookies to improve your experience. Do you agree with that? or a phrase like this. We usually click " yes" without thinking because we want to see the content. but should we accept cookies?

Accepting cookies can create serious security risks; since cookies are stored on the hard disk as text files, any intruder can easily open these files and view the information. Additionally, all sites that collect information from cookies are not legitimate. Some of them can use cookies for hacking purposes. However, in this article, we are looking for an answer to the question of whether the use of cookies can violate our privacy. And how?

2. Methodology

The present research has been done using the descriptive-analytical method and by studying various documents and sources. Data collection was through library research, legal research centers, and access to books, articles, theses, journals, and websites.

3. Results and Discussion

Nowadays, cyberspace has made it easier than ever to violate privacy, which is closely related to the personality of people; In such a way that criminals attack human life in all parts of the world, regardless of geographical boundaries, away from the controlling eyes and gaze of others and free from the inspection and surveillance of others. With the advent of computer technology, it is possible to plan and violate privacy and steal private and confidential information of individuals more than in the past with very high accuracy and clarity. (Qanad and Alighli, 2020, 306)

Cookies play an essential role in enhancing user experience and facilitating personalized interactions on the web. However, behind their harmless appearance, there is a domain full of possible dangers and harms that may endanger the user's privacy and security.

Although cookies can be blocked as said earlier some websites become not as effective when we don't accept them. Some of us simply use the websites and to get the full functionality accept the cookies unwillingly and are concerned about our privacy and tracking. (Jegatheesan, 2013, p. 2)

Cookies are set by the websites we visit or even sometimes by the third-party websites that involve in marketing, ad serving. There are even chances that we get cookies from websites we have never heard of or never visited but those websites are associated with the websites we visit. These websites do various activities like advertising, help in marketing the brand or product, increase revenue or even track the users. These websites may set cookies that can track the movement of users from one website to another website and can consolidate the personal data and sometimes making it available for anyone with commercial interest. And this is where we have to worry about the invasion of privacy, because the information collection cookies are not nearly as obvious, and the websites don't simply stop at tracking, they start showing adverts, campaigns are done around you to force you to buy or look at something for the fact that you had once of frequently interested in something. This eliminates the ability for us to look for new things, in simple ways we are restricted from being shown something new and we are always shown the same things, given preferences of something we did already. (Ibid, 2013, p. 3) Tracking cookies can actually be a threat to user privacy. Because tracking cookies collect data about people's behavior on

the Internet, it is absolutely essential for website owners to allow their users control over which cookies they accept. According to the General Data Protection Regulation (GDPR), every web user must have the option to accept or reject cookies when browsing the Internet. And if any website does not provide this option to its users, it violates the general data protection regulations.

Also, according to the general data protection regulations, users have rights in relation to their personal data, such as the right to access, modify, limit, withdraw consent, protest, portability, and erasure. In addition, they have the right to object to automatic decision-making profiling, and processing of their personal data for direct marketing. (Article 15-22)

Another concern with cookies is security issues with cookies. When they are manipulated by malicious entities, they also pose a significant threat. Attackers can use various techniques such as session hijacking, cross-site scripting, cross-site request forgery, etc. to abuse cookies in malicious activities. (Layeeq, 2024, p. 3)

The current uses of cookies tell us why users should be concerned about their privacy being violated.

When a user enters the Internet and registers his name or fills out a form online, he actually makes a profile of his personal information available to various companies. Many companies also use cookies to collect personal information of users and make profiles. In fact, companies do not use personal information only to provide products or services, they also use this information in various political and social cases. Awsat et al., (2020, 1354)

"The author of "Four Ethical Issues of the Information Age," talks about how profiling violates privacy when he states: "You or I may have contributed information about us freely to each of the separate databases but that by itself does not amount to giving consent to someone to merge the data. (Mason, 1986, pp. 5 - 12)

Websites and companies that conduct online marketing through cookies must have clear policies and provide clear options to individuals on how to store, use, or transfer personal information. This increases the informed choice of users regarding their consent for any activity, correct and free use of the Internet space. Providing clear opt-outs allows people to exercise control when using online web services. Some people may want to visit a website without any record of their online behavior being kept. So it's a good idea to provide a simple tool to opt out of ad targeting using behavioral data. It's a legal requirement under privacy and electronic communications laws to tell a person when information is going to be stored on their device, For example, in the form of a regular cookie, or a flash cookie, and give him the opportunity to refuse this. It is also a good idea to give users relevant advice on how to use their web browser settings or the choices provided on the website itself to allow the user to maintain their online anonymity. For example, by ensuring that their identifying information is deleted at the end of a session or any other similar solution.

4. Conclusion

In the broad landscape of digital technology, cookies play an essential role in enhancing the user experience and facilitating personalized interactions on the web. However, behind their harmless appearance, there is a large volume of potential risks and harms such as tracking and profiling, challenges related to cookie management, and security risks that can endanger the privacy and security of users.

As discussed so far, there are two main risks from cookies that affect all other risks; One risk is invasion of privacy and the second risk is security vulnerability. Cookies can track our online activities on different websites over time and create a profile of our interests and preferences. This information can be used by advertisers to target us with personalized ads, or the data can be sold to third parties without our consent. Personal data and its processing are not permitted without obtaining the express consent of the person, and if permission is obtained, it can be used only for the purpose of the person's consent.

Regarding security vulnerabilities, it should be said that in some cases user data and communications may be used by governments for the benefit of national security or any other similar concern. But there are other ways that our data may be misused and stolen. Where cybercriminals and hackers can exploit cookies to access our account

information or steal sensitive data through a process called cross-site scripting. Additionally, hackers execute or inject malicious scripts into a trusted program or file, such as a cookie, to do their nasty work. However, when viewing cookies, users always have a concern and a feeling of insecurity about violating their privacy and stealing their information. In general, it seems that there is a possibility of violating privacy and compromising personal data with cookies on a small scale.





حقوق فناوری‌های نوین

<http://doi.org/10.22133/mtlj.2025.467629.1352>

کوکی‌ها و قابلیت تجاوز به حریم خصوصی در فضای سایبر

فرنگیس منصوری 

استادیار، گروه حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله	چکیده
مقاله پژوهشی تاریخ دریافت: ۱۴۰۳/۰۳/۲۳ تاریخ پذیرش: ۱۴۰۳/۰۵/۱۷ واژگان کلیدی: کوکی حریم خصوصی امنیت اطلاعات شخصی فضای سایبر *نویسنده مسئول رایانامه: f.mansoori@pnu.ac.ir	امروزه حفظ حریم خصوصی در فضای مجازی نگرانی‌ای عمده برای مردم جهان است. برخی از وبسایت‌ها با استفاده از نبود نهادی واحد که بتواند فضای آنلاین را با قوانین محدودکننده و سختگیرانه خود اداره کند، از فایل‌های متنی به نام کوکی در جمع‌آوری داده‌ها از کاربران و استفاده از آن‌ها برای بازاریابی‌شان در شبکه‌های تبلیغاتی و وبسایت‌های شخص ثالث با کمک فناوری‌های مختلف استفاده می‌کنند. ممکن است استدلال شود که این نوعی راهبرد بازاریابی است و در بیشتر موارد خطرناک نیست، اما می‌تواند به نگرانی‌های امنیتی و نقض حریم خصوصی منجر شود؛ زیرا اکثر وبسایت‌ها برای استفاده از کوکی‌ها و تنظیم آن‌ها در مرورگر کاربر مجوز نمی‌خواهند. سؤال اصلی در این مقاله این است که کوکی‌ها چگونه و تا چه حد می‌توانند حریم خصوصی کاربران را نقض کنند؟ در پاسخ به این پرسش به روش توصیفی و تحلیلی و با استفاده از منابع کتابخانه‌ای و اینترنتی خواهیم گفت که اگرچه کوکی‌ها در چشم‌انداز وسیع فناوری دیجیتال، نقشی اساسی در افزایش تجربه کاربر و تسهیل تعاملات شخصی‌شده در وب دارند، با این حال همچنین با خطراتی همراه هستند که کاربران باید از آن آگاه باشند. در مجموع دو خطر اصلی وجود دارد؛ یکی تجاوز به حریم خصوصی کاربران و دومین خطر، آسیب‌پذیری امنیتی.

نحوه استناددهی: منصوری، فرنگیس (۱۴۰۴). کوکی‌ها و قابلیت تجاوز به حریم خصوصی در فضای سایبر. حقوق فناوری‌های نوین، ۶(۱۱)، ۳۷۷-۳۹۵.

ناشر: دانشگاه علم و فرهنگ <https://www.usc.ac.ir>

شاپای الکترونیکی: ۲۷۸۳-۳۸۳۶

مقدمه

همه افرادی که آنلاین هستند دوست دارند حریم خصوصی داشته باشند و این انتظار منطقی است. کوکی‌های اینترنتی فایل‌های متنی کوچکی هستند که برای تبادل اطلاعات بین مرورگر کاربر و وبسایت طراحی شده‌اند و توسط سایت‌هایی که از آن‌ها بازدید می‌کنید اطلاعاتتان را ذخیره می‌کنند. کوکی‌ها شامل انواع اطلاعات لازم برای پیمایش در وبسایت مدنظر هستند. به همین دلیل، برای شرکت‌های تجارت الکترونیک و آژانس‌های تبلیغاتی بسیار مهم‌اند. تقریباً در اکثر وب‌گردی‌ها، یک اعلان به ما داده می‌شود که «این وبسایت از کوکی‌ها برای بهبود تجربه شما استفاده می‌کند. موافقت می‌کنید؟» یا عبارتی مشابه این. معمولاً بدون فکرکردن روی بله کلیک می‌کنیم؛ چون می‌خواهیم محتوا را ببینیم، اما آیا باید کوکی‌ها را قبول کنیم؟

پنجره‌هایی که صرفاً با قبول کردن کوکی‌ها باز می‌شوند یکی از بزرگ‌ترین مزاحمت‌های اینترنتی هستند. از آنجاکه کوکی‌ها در هارد دیسک به صورت فایل متنی ذخیره می‌شوند، خطرات امنیتی جدی به همراه دارد. هر مزاحمی می‌تواند به راحتی این فایل‌ها را باز کند و اطلاعات را مشاهده کند. همچنین همه سایت‌هایی که اطلاعات را از کوکی‌ها جمع‌آوری می‌کنند قانونی نیستند. برخی از آن‌ها، که از کوکی‌ها به منظور هک استفاده می‌کنند، ممکن است مخرب باشند.

در چهارچوب هدف‌گذاری رفتاری، اطلاعات پیوند داده شده از طریق کوکی‌ها برای پروفایل سازی کاربر استفاده می‌شود و با توجه به این پروفایل، آگهی‌هایی برای کاربر ارسال می‌شود که احتمالاً به آن‌ها علاقه دارد، اما این موضوع درمورد حضور آنلاین، حریم خصوصی و امنیت داده‌های شخصی پیامدهایی بسیار جدی دارد. بسیاری از مردم هنوز از این نوع فعالیت‌های وبسایت‌های هوشمند بی اطلاع هستند. این وبسایت‌ها درمورد کاربران اطلاعات کافی به دست می‌آورند. سپس بازاریابی خود را با کمک کوکی‌ها شروع می‌کنند و فقط آنچه وبسایت فکر می‌کند کاربر به آن نیاز دارد نشان می‌دهند یا ممکن است اطلاعات را به شخص ثالث انتقال دهند. این نقض آشکار حریم خصوصی و امنیت داده‌هاست.

در فضای مجازی، حفظ حریم خصوصی مهم‌ترین نگرانی است. کوکی‌ها نمی‌توانند مانند ویروس‌ها به رایانه آسیب برسانند (Peng & Cisna, 2000, p. 150). آن‌ها فقط فایل‌های متنی هستند که داده‌ها را از سرورهای وب ذخیره می‌کنند، اما اکثر وبسایت‌ها، گزینه پذیرش یا رد کوکی‌ها را ارائه نمی‌دهند که کاربر حق انتخاب داشته باشد. برخی از وبسایت‌ها به کاربران اجازه نمی‌دهند که از وبسایت بازدید کنند یا اقدامی را انجام دهند؛ فقط به این دلیل که استفاده از کوکی‌ها را رد کرده‌اند. حتی آن‌ها به خوبی می‌دانند که این امر بر چشم‌انداز کسب و کارشان تأثیر می‌گذارد. به هر حال ما در این مقاله به دنبال پاسخ به این سؤال هستیم که آیا استفاده از کوکی‌ها قابلیت نقض حریم خصوصی ما را دارند؟ و چگونه؟

۱. حریم خصوصی

در حال حاضر دو نوع حریم خصوصی وجود دارد: اولین مورد حریم خصوصی در زندگی واقعی است که به عنوان حداقل سطح نفوذ به فضای فیزیکی یا تنهایی تعریف می‌شود. دومین مورد حفظ حریم خصوصی در محیط مجازی است که به عنوان فضای سایبری نیز شناخته می‌شود و به جمع‌آوری اطلاعات کاربران از منابع متعدد از جمله اینترنت اشاره دارد. جمع‌آوری اطلاعات، پردازش، انتشار و نقض داده‌های خصوصی همگی نمونه‌هایی از حریم خصوصی و جنبه‌های مربوط به آن در دنیای مجازی هستند (Rerru Singh, 2022, p. 26).

حریم خصوصی جزو بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی می‌شود که ارتباط تنگاتنگی با شخصیت انسان دارد؛ به گونه‌ای که تجاوز به آن، تجاوز به شخصیت و کرامت انسانی است. حریم خصوصی به لحاظ مفهوم لغوی از دو واژه حریم و خصوصی تشکیل شده است. حریم به معنای محدوده معقوله است که فرد انتظار دارد از دسترس دیگری مصون بماند. این دیگری هم می‌تواند دولت باشد و هم سایر

اشخاص حقیقی و حقوقی. حریم در لغت از ریشه «حرم» است و حرم به معنای محدوده، بازداشته‌شده، گرداگرد، دوروبر و اطراف است (Ansari, 2004, p. 842).

ارائه تعریفی جامع و مانع از حریم خصوصی امری نسبی است؛ زیرا حریم خصوصی با توجه به شرایط اقتصادی، اجتماعی، فرهنگی و مذهبی از زمانی به زمانی دیگر و همچنین از جامعه‌ای به جامعه‌ای دیگر متفاوت است. به همین دلیل، در تعریف این مفهوم باید گستره آن را منعطف در نظر گرفت تا توان انطباق با تغییرات را داشته باشد (Shahbazi & Shabani Kolahi, 2024, p. 225). به‌طورکلی در فرهنگ‌های گوناگون، تعاریف و برداشت‌های مختلفی از حریم خصوصی وجود دارد. حریم خصوصی تأیید ذاتی تنوع، حق فرد برای متمایز بودن و ایجاد منطقه انفرادی در مخالفت با موج شباهت است. حریم خصوصی شخص را در برابر چشمان کنجکاو عمومی در مفاهیمی که برای او شخصی است محافظت می‌کند. حریم خصوصی به افراد مربوط می‌شود تا مکانی که آن‌ها به آن وابسته‌اند. از آنجاکه فرد می‌تواند انتخاب کند چگونه از آزادی در حریم خصوصی به بهترین شکل بهره می‌برد، حریم خصوصی سنگ بنای همه آزادی‌هاست. کرامت فردی و حریم خصوصی درهم تنیده شده‌اند (Rerru Singh, 2022, p. 25).

حقوق‌دانان نیز تعاریف متعددی از حریم خصوصی ارائه داده‌اند که برخی از آن‌ها عبارت‌اند از: حق بر تنهاماندن؛ دسترسی محدود دیگران به انسان و توانایی ایجاد مانع در برابر دسترسی ناخواسته و ناخوانده به انسان؛ محرمانگی و پنهان‌ساختن برخی امور از دیگران؛ کنترل بر اطلاعات شخصی؛ حمایت از شخصیت و کرامت؛ حق بر عالم صمیمیت و کرامت انسان‌ها (Hessam et al., 2021, p. 72). در تعریفی کامل‌تر «حریم خصوصی» را قلمروی از زندگی انسان دانسته که نوعاً یا عرفاً یا شخصاً رضایت ندارد دیگران او را در آن قلمرو به انحاء مختلف مورد تعرض قرار دهند (Ansari, 2022, p. 154).

در بند اول ماده ۲ لایحه حریم خصوصی که در زمان دولت هفتم به مجلس ارائه شد، در تعریف حریم خصوصی مقرر می‌دارد: «حریم خصوصی قلمروی از زندگی هر شخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد دیگران بدون رضایت وی بدان وارد نشوند یا بر آن نظارت نکنند، یا به اطلاعات راجع به آن دسترسی نداشته باشند، یا آن قلمرو را مورد تعرض قرار ندهند. جسم، البسه، و اشیاء همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند.» بند پ ماده ۱ آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، حریم خصوصی را قلمرویی از زندگی شخصی فرد معرفی کرده است که انتظار دارد دیگران بدون رضایت یا اعلام قبلی وی یا به حکم قانون یا مراجع قضایی آن را نقض نکنند؛ از قبیل حریم جسمانی، واردشدن، نظاره‌کردن، شنود و دسترسی اطلاعات شخصی فرد از طریق رایانه، تلفن همراه، نامه، منزل مسکونی، خودرو و آن قسمت از مکان‌های اجاره‌شده خصوصی نظیر هتل و کشتی همچنین آنچه حسب قانون، فعالیت حرف‌های خصوصی هر شخص حقیقی و حقوقی محسوب می‌شود؛ از قبیل اسناد تجاری و اختراعات و اکتشافات.

حریم خصوصی اطلاعاتی به معنای حق اولیه افراد در محرمانه‌ماندن اطلاعات شخصی و ممانعت از تحصیل، پردازش و انتشار غیرقانونی داده‌های شخصی مربوط به ایشان است. حمایت از داده‌های شخصی مربوط به ایشان از جمع‌آوری، پردازش و افشای غیرقانونی است؛ زیرا اشخاص اصولاً داده‌های شخصی خود را قلمرو اختصاصی و ممنوع از تعرض تلقی می‌کنند (Masoudi, 2019, p. 14). طبق بند ب ماده ۱ قانون انتشار و دسترسی آزاد به اطلاعات، منظور از «اطلاعات شخصی، اطلاعات فردی نظیر نام و نام خانوادگی، نشانی‌های محل سکونت و محل کار، وضعیت زندگی خانوادگی، عادت‌های فردی، ناراحتی‌های جسمی، شماره حساب بانکی و رمز عبور است.»

طبق بند الف ماده ۱ آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات، به هر نوع داده از جمله صوت، تصویر، فیلم، نوشته، نشانه، نقشه، اعداد و یا ترکیبی از آن‌ها که در اسناد مندرج باشد یا به صورت نرم‌افزاری ذخیره شده یا با هر وسیله دیگری ضبط شده باشد، داده یا اطلاعات می‌گویند. طبق بند ب همان آیین‌نامه، به اطلاعات مربوط به هویت، احوال شخصی، وضعیت فردی، عقاید و باورها، پست

الکترونیکی، عکس و فیلم و صوت و تصاویر و عادات رفتاری و فردی از قبیل نام و نام خانوادگی، محل و تاریخ تولد، ازدواج، طلاق، مشخصات همسر، والدین و فرزندان، نسبت خانوادگی، ناراحتی‌های جسمی و روحی، شماره حساب بانکی و رمز عبور، محل کار و سکونت و همچنین اطلاعات شخصی مربوط به انجام امور تجاری، شغلی، تحصیلی، مالی، آموزشی، اداری، پزشکی و حقوقی اطلاعات شخصی گفته می‌شود. در اعلامیه «کنفرانس حقوق دانان درباره حریم خصوصی»^۱، که در سال ۱۹۷۶ در نروژ برگزار شد، در تعریف حریم خصوصی این گونه تصریح کرده است: حق حریم خصوصی حقی است نسبت به تنه‌اماندن، زندگی کردن با سلیقه خود و با حداقل مداخله دیگران. همچنین در این کنفرانس بر صیانت از فرد در برابر ورود و مداخله دیگران، صداپرداری و تصویربرداری پنهانی از وی یا استراق سمع ارتباطات او، استفاده از مواد و مطالبی که با ورود غیرقانونی به حریم خصوصی فرد به دست آمده است یا هویت شخص را آشکار می‌سازد یا از او چهره‌ای کاذب ارائه می‌دهد یا وقایع خصوصی آزاددهنده او را افشا می‌سازد، تأکید شده است (Masoudi, 2019, p. 13).

شورای اروپا نیز در قطعنامه ۴۲۸ مورخ ۱۹۷۰^۲ در تعریف حریم خصوصی اعلام می‌کند که حق حریم خصوصی، مربوط می‌شود به زندگی خصوصی، خانوادگی و مسکن، تمامیت جسمی و روحی، آبرو، اعتبار و شهرت و حیثیت افراد، اجتناب از این که چهره‌ای کاذب از فرد ساخته شود، افشانکردن وقایع و حقایق نامربوط و آزاددهنده، عدم افشای غیرمجاز تصاویر خصوصی، حمایت از عدم افشای اطلاعاتی که برائت اعتماد، اشخاص وصول کرده‌اند یا در اختیار آن‌ها قرار گرفته است (Masoudi, 2019, p. 13). آنچه اهمیت دارد حفاظت از اصول اساسی حریم خصوصی در قوانین ملی و قوانین بین‌المللی است. در حوزه بین‌المللی، سه سند بین‌المللی وجود دارد که به منزله مبنای حمایت از حریم خصوصی و زندگی شخصی شناخته شده است: ماده ۱۲ اعلامیه جهانی حقوق بشر ۱۹۴۸^۳، ماده ۱۷ میثاق بین‌المللی مدنی و حقوق سیاسی^۴ ۱۹۶۶ و ماده ۸ کنوانسیون اروپایی حقوق بشر^۵؛ البته بند ۱۸ اعلامیه حقوق بشر تهران مصوب ۱۹۶۸ و دستورالعمل‌های سازمان همکاری اقتصادی و توسعه^۶ در مورد حفاظت از حریم خصوصی و جریان فرامرزی داده‌ها نیز مرتبط‌اند.^۷

در این اسناد، دو نوع تعهد برای دولت‌ها در نظر گرفته شده است: نخست این که دولت‌ها مکلف‌اند در زمینه حریم خصوصی، اقدامات ایجابی انجام دهند و دیگر این که ملزم شده‌اند اقدامات سلبی لازم را در خصوص مداخله‌نکردن در حریم خصوصی ایجاد کنند (Maghmi & Attaran, 2018, p. 315).

شورای حقوق بشر و مجمع عمومی سازمان ملل در سال‌های ۲۰۱۲ تا ۲۰۱۶ قطعنامه‌هایی را در خصوص حریم خصوصی در عصر دیجیتال به تصویب رساندند و مقرر داشتند که قواعد مربوط به حقوق بشر در فضای فیزیکی برای فضای سایبر نیز اعمال شود. در اعلامیه حقوق بشر سازمان ملل (بازبینی ۲۰۱۳)^۸، سازمان ملل به اتفاق آرا حق حفظ حریم خصوصی اطلاعاتی افراد را به منزله یکی از حقوق اساسی بشر پذیرفت. براین اساس، هرگونه ارتباطات برخط افراد محترم بوده و حفظ می‌شود، قوانین ملی باید ضمن جلوگیری از تجاوز به حریم خصوصی انسان‌ها، با حق حفظ این حریم سازگاری داشته باشند و سازوکارهایی برای شفافیت عملکرد دولت‌ها در نظارت بر انتقال داده‌ها تعریف شود (Nekonom, 2024, p. 30).

قطعنامه ۱۶۶ / ۶۹ نیز با این هدف، کشورها را به اصلاح قوانین و مقررات خود در خصوص جمع‌آوری و نگهداری اطلاعات شخصی ملزم کرد و تأکید داشت که دولت‌ها تحت لوای قواعد بین‌المللی حقوق بشر به تعهدات خود عمل کنند. قطعنامه ۱۶ / ۲۸ در سال ۲۰۱۵ نیز خواستار ارائه روشی مؤثر برای شناسایی اصول، استانداردها و شیوه‌های بهینه حفاظت از حریم خصوصی شد تا با تدوین قوانین و مقررات همسو

1. Nordic Conference of Jurists on the Right to Respect for Privacy, 1976.

2. Resolution 428 of the Consultative (Parliamentary) Assembly of the Council of Europe -1970.

3. Universal Declaration of Human Rights

4. International Covenant on Civil and Political Rights, 1966.

5. European Convention on Human Rights

6. Organization for Economic Co-operation and Development

7. <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe protectionofprivacy and transborderflowsofpersonaldata. html>

8. United Nations Declaration of Human Rights (revision in 2013)

با موازین بین‌المللی حقوق بشر، دستاورد مطلوب در صیانت از حقوق شهروندی در فضای سایبر حاصل آید. (Raeesi & Qasimzadeh, 2019, pp. 128-129)

اتحادیه اروپا در سال ۲۰۱۶، با بازنگری سند ۹۵ / ۴۶ / EU سال ۱۹۹۵، بر حمایت افراد در برابر پردازش داده‌های شخصی و انتقال آن تأکید کرد و برابر این سند، حق استفاده و پردازش داده‌های شخصی، بدون کسب رضایت صریح شخص، غیرمجاز است و در صورت کسب اجازه هم صرفاً برای هدف مورد رضایت شخص، می‌تواند بهره‌برداری شود که مفاد این سند، با استقبال اکثر کشورهای جهان، به‌استثنای کشورهای معدودی، از جمله آمریکا همراه شد و آن کشورها، قوانین و مقررات خود را در حمایت از داده‌های شخصی، مطابق با این سند تصویب یا اصلاح کردند (Raeesi & Qasimzadeh Liasi, 2019, p. 130). همچنین اتحادیه اروپا مقررات حفاظت از داده‌های عمومی^۱ را با هدف تقویت حمایت از داده‌ها، در ماه می ۲۰۱۸ تصویب کرد که به‌موجب آن، کلیه دولت‌های عضو بدون نیاز به قانون‌گذاری مجدد، به رعایت قواعد مندرج در مصوبه مکلف شده‌اند.

اصل پنجم «مشور حقوق بشر و اصول ناظر به اینترنت»^۲ بیان می‌دارد: «همه افراد حق برخورداری از حریم خصوصی آنلاین را دارند. این شامل عدم نظارت، حق رمزگذاری داده‌ها^۳ و حق گمنامی آنلاین می‌شود. همچنین حق حفاظت از داده‌ها که شامل کنترل بر اطلاعات شخصی، نگهداری، پردازش، دفع و افشا است، باید محترم شمرده شود.»

در نظام حقوقی ایران اما تاکنون قانون مستقلی درخصوص حریم خصوصی و مسائل مرتبط با آن وضع نشده و حتی در قانون اساسی به‌منزله مهم‌ترین قانون کشور باز هم اصل یا اصولی به‌صورت خاص و صریح در حمایت از حریم خصوصی دیده نمی‌شود.^۴ در برخی اصول قانون اساسی حمایت از حریم خصوصی، به‌صورت ضمنی تحت عناوینی مانند حریم خلوت و تنهایی، حریم مکانی، حریم اطلاعات، حریم ارتباطات و حریم جسمانی وجود دارد. در قانون مجازات اسلامی، قانون جرائم رایانه‌ای و برخی قوانین دیگر هم مواردی به‌صورت پراکنده مشاهده می‌شود؛ البته در حوزه حمایت از داده‌ها در فضای سایبر، قانون تجارت الکترونیک مصوب ۱۳۸۲، تاحدودی فقدان قانون ویژه حمایت از حریم خصوصی و داده‌ها را جبران می‌کند.

به‌هرحال دولت‌ها باید با وضع قوانین مناسب و مجازات‌های بازدارنده و مؤثر، از نقض حق حریم خصوصی شهروندان و تخریب و دست‌کاری داده‌ها در فضای سایبر جلوگیری کنند.

۲. نقض حریم خصوصی در فضای سایبر

نقض حریم خصوصی در فضای مجازی یکی از مهم‌ترین مسائل روز نه تنها در جامعه ما بلکه در دنیاست. در کنار مزیت‌های گسترده‌ای، که این فضا به همراه دارد، استفاده نادرست از آن پیامدهای نامطلوبی را نیز به‌دنبال دارد که یکی از آن‌ها نقض حریم خصوصی افراد با استفاده از این فناوری‌ها از سوی برخی اشخاص و سازمان‌ها یا حتی دولت‌هاست که با اهدافی متفاوت صورت می‌گیرد. (Qanad & Aligli, 2019, p. 298).

زمانی حریم خصوصی حاکی از این بود که افراد می‌توانند تنها و منزوی باشند، اما این امر از اساس تغییر کرده است. موانع لجستیکی ایجادشده از طریق جغرافیا زمانی از شخص محافظت می‌کرد، ولی این نیز به‌شدت تغییر کرده و دیوار حفاظتی جغرافیایی با توسعه اینترنت و از طریق شبکه جهانی وب برداشته شده است. امروزه دیگر نمی‌توان حریم خصوصی را حتی در خانه خود، امن فرض کرد (Tripathi, 2020, p. 14).

1. General Data Protection Regulation "GDPR"

2. The Charter of Human Rights and Principles for The Internet, UN Internet Governance Forum, 2011.

3. Encryption

۴. باین حال مفهوم حریم خصوصی را می‌توان به‌طور ضمنی از برخی اصول قانون اساسی استنباط کرد: اصول ۴۲ و ۴۰، ۳۹، ۳۸، ۳۵، ۳۳، ۳۲، ۳۰، ۲۸، ۲۷، ۲۶، ۲۵، ۲۴، ۲۳، ۲۲، ۲۰، ۱۹. ر.ک: سیدمحمد هاشمی، حقوق اساسی جمهوری اسلامی ایران، ج ۲، نشر میزان.

امروزه فضای مجازی تجاوز و تعدی به حریم خصوصی را، که با شخصیت افراد ارتباط تنگاتنگ دارد، بیش از پیش آسان کرده است؛ به گونه‌ای که مجرمان در اقصی نقاط جهان، فارغ از مرزهای جغرافیایی، به دور از چشم و نگاه کنترل‌کننده دیگران و رها از تفتیش و تجسس دیگران، به زیستن انسان تعرض می‌کنند. با ظهور فناوری رایانه‌ای، امکان طرح‌ریزی و هتک حریم خصوصی و سرقت اطلاعات سری و خصوصی اشخاص بیش از گذشته فراهم شده است. همچنین اگر پیش از این جاسوسان اطلاعات با مشکلاتی مواجه بودند، این سیستم‌ها امکاناتی فراهم کرده‌اند که در کمترین زمان ممکن و با دقت و وضوح بسیار بالا اطلاعات سری و غیرسری مدنظر خود را به دست آورند. همچنین سیستم‌های رایانه‌ای این امکان را فراهم آورده که مجرمان در ورای مرزها و اقصی نقاط جهان، اطلاعات دیگران را بدون اینکه خودشان متوجه شوند سرقت کنند و ارزش ذاتی آن را از بین ببرند و از حالت خصوصی و سری بودن خارج کنند. رایانه همچون تیغی است که منحرفان اجتماعی از لبه تیز آن علیه بشریت استفاده می‌کنند (Qanad & Alighli, 2019, p. 306).

به‌هرحال نقض حریم خصوصی از دو منظر قابل بررسی است. یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضان حریم خصوصی در فضای مجازی.

بزه‌دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می‌کنند. بسیاری از بزه‌دیدگان جرایم سایبری و کسانی که حریم خصوصی‌شان در فضای مجازی نقض می‌شود، استعدادی درخور توجه برای قربانی شدن بروز می‌دهند و به‌راحتی طعمه بزهکاران سایبری می‌شوند. ضعف شخصیتی، فقدان اطلاعات کافی درباره محیط مجازی و بی‌دقتی در محافظت از داده‌ها مواردی است که قربانی بزه سایبری را در قربانی شدنش مساعدت می‌کند. اشخاص باید در قبال صیانت از حریم خصوصی خود همت کنند. بسیاری اشخاص بدون رعایت مسائل امنیتی، خصوصی‌ترین اطلاعات خود را بر روی سیستم رایانه‌ای یا حامل‌های داده نظیر فلش و کارت‌های حافظه و تلفن همراه و سی‌دی ذخیره می‌کنند و به‌نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می‌گذارند و این چنین استعداد قربانی شدن در فضای مجازی را از خود نشان می‌دهند (Fathi & Shahmoradi, 2016, p. 241).

جنبه دیگر موضوع مربوط به ناقضان حریم خصوصی در فضای مجازی است. این بزهکاران زمانی که وارد فضای مجازی یا همان اینترنت می‌شوند آن را ملک طلق خود تلقی می‌کنند و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می‌دهند. بعضی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه‌ای جرم‌انگاری شده عبارتند از:

- ۱) دسترسی غیرمجاز به داده‌های رایانه‌ای یا مخابراتی نظیر هک ایمیل یا اکانت اشخاص؛
- ۲) شنود غیرمجاز محتوای درحال انتقال در سیستم‌های رایانه‌ای یا مخابراتی نظیر استفاده از نرم‌افزارهای شنود چت‌های اینترنتی؛
- ۳) دسترسی غیرمجاز به داده‌های سری درحال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده یا تحصیل و شنود آن؛
- ۴) در دسترس قرار دادن داده‌های سری درحال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده برای اشخاص فاقد صلاحیت؛
- ۵) نقض تدابیر امنیتی سیستم‌های رایانه‌ای یا مخابراتی به قصد دسترسی به داده‌های سری درحال انتقال در سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده؛
- ۶) حذف یا تخریب یا مختل یا غیرقابل پردازش کردن داده‌های دیگری از سیستم‌های رایانه‌ای یا مخابراتی یا حامل‌های داده به‌طور غیرمجاز؛
- ۷) از کار انداختن یا مختل کردن سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز نظیر غیرفعال‌سازی دیتابیس تارنماها و ممانعت از دسترسی اشخاص به پایگاه اینترنتی‌های شخصی؛
- ۸) ممانعت از دسترسی اشخاص مجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی به‌طور غیرمجاز؛
- ۹) ربودن داده‌های متعلق به دیگری به‌طور غیرمجاز؛
- ۱۰) هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف‌شده دیگری از طریق سیستم‌های رایانه‌ای یا مخابراتی؛

(۱۱) نشر اکاذیب از طریق سیستم های رایانه ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی. انتشار غیرمجاز گذرواژه یا هرگونه داده شخصی در فضای مجازی، اقدامی است که اغلب به دلایلی همچون افسردگی، عصبانیت، حسادت یا انتقام جویی صورت می گیرد. این افراد به دلایل مختلفی از جمله تفریح، سرگرمی، خودکم بینی، حس رقابت و بی توجهی به اصول اخلاقی، خود را مجاز می دانند تا به حریم خصوصی دیگران تجاوز کنند. این عمل می تواند خسارات جبران ناپذیری از جمله لطمه به حیثیت، زیان های مالی و حتی تهدید جانی برای قربانیان به همراه داشته باشد (Fathi & Shahmoradi, 2016, pp. 241-244).

۳. کوکی و انواع آن

کوکی ها فایل های متنی با داده های کوچکی مانند نام کاربری و رمز عبورند که برای شناسایی رایانه کاربر هنگام استفاده از شبکه استفاده می شوند. به عبارت دیگر، کوکی مرورگر در واقع بسته ای از اطلاعات است که در قالب یک فایل متنی توسط وبسایت ها روی رایانه و (موبایل) کاربر ذخیره می شود تا از طریق آن کاربر شناسایی شده و مثلاً بدون نیاز به ورود نام کاربر و رمز عبور همواره در سایت لاگین باقی بماند (Yusefnejad & Taheranpour, 2022, p. 1).

۱-۳. انواع کوکی ها

کوکی ها بسته به نوع کاربردی که دارند چند نوع اند:

۱. کوکی های جلسه^۱

کوکی های جلسه مختص مدتی هستند که کاربر در حال پیمایش داخل یک وبسایت است؛ بنابراین وقتی نشست یا در واقع پیمایش کاربر تمام می شود، این کوکی ها هم پاک می شوند. این مورد از انواع کوکی روی هارددیسک نگهداری نشده و فقط روی رم ذخیره می شوند.

۲. کوکی های دائمی^۲

کوکی های دائمی یا پایا با دو هدف احراز هویت و ردیابی طراحی شده اند؛ کوکی های احراز هویت، مختص ذخیره کردن اطلاعات ورودند، اما کوکی های ردیابی، نحوه پیمایش کاربر را ردیابی می کنند تا نیازهای او را شناسایی کنند. پیشنهاد محصولات مرتبط با جست و جوی های اخیر، مثالی از کاربردهای این کوکی هاست. این اطلاعات بعد از بستن مرورگر حذف نمی شوند. ضمن این که خود وبسایت می تواند این اطلاعات را به روز کند.

۳. کوکی های موقت^۳

کوکی های موقت با خارج شدن از وبسایت پاک می شوند. درواقع کوکی های جلسه از این نوع کوکی هستند؛ البته این کوکی ها این قابلیت را هم دارند که یک تاریخ انقضا بگیرند. دراین صورت، این کوکی ها با خروج از مرورگر پاک نمی شوند، اما می توانند به روز شوند.

۴. کوکی های زامبی^۴

از ترکیب انواع کوکی شخص ثالث و پایا، «کوکی زامبی» تشکیل می شود. دلیل این نام گذاری آن است که حتی اگر حذفشان کنید، باز به مرورگر برمی گردند. چون در جایی به غیر از محل اصلی ذخیره کوکی ها یا در مکان های امن مرورگر ذخیره شده اند، اما چرا بعضی وبسایت ها از این کوکی استفاده می کنند؟ گاهی اوقات این کوکی ها توسط هکرها ساخته شده و برای آلوده کردن سیستم شما به ویروس و بدافزار استفاده می شوند. اما بعضی وبسایت ها هم با هدف رصد کردن فعالیت کاربران، این کوکی اینترنتی را طراحی می کنند.

1. Session Cookies
2. Persistent Cookies
3. Temporary Cookies
4. Zombie Cookies

۵. کوکی‌های شخص اول^۱ و کوکی‌های شخص ثالث^۲

یکی از مباحث مهم درباره کوکی‌ها، دسترسی وبسایت‌ها به آن‌هاست. کوکی‌ها هم می‌توانند فقط از طریق وبسایتی که اطلاعاتشان به آن تعلق دارند دسترسی‌پذیر باشند و هم می‌توانند از طریق وبسایت‌های دیگر دسترسی‌پذیر باشند. بر همین اساس، کوکی‌ها به دو دسته شخص اول و شخص ثالث تقسیم می‌شوند. در کوکی شخص اول، اطلاعات فقط بین مرورگر و وبسایت اول (وبسایت اصلی) قابلیت تبادل دارند؛ بنابراین امنیت بالایی هم دارند. برعکس کوکی‌های شخص ثالث متعلق به وبسایت دیگری با دامنه‌ای متفاوت‌اند. برای مثال کاربر وارد وبسایت flowers-shop.com می‌شود و یکسری کوکی از این وبسایت داخل مرورگرش ذخیره می‌شود، اما این وبسایت از طریق تبلیغاتی که نشان می‌دهد، با دامنه web-adds.com در ارتباط است. در این میان، web-adds.com هم از مرورگر کاربر می‌خواهد که کوکی‌هایی را ذخیره کند. به این ترتیب، دامنه دوم هم می‌تواند فعالیت کاربر را ردیابی کند و به همین سادگی، بحث امنیت اطلاعات و حریم خصوصی کاربران وب تهدید می‌شود^۳ (Borzoudi, 1403, p. 2).

۲-۳. معایب و مزایای کوکی‌ها

کوکی‌ها در افزایش تجربه کاربر و تسهیل تعاملات شخصی‌شده در وب، نقشی اساسی دارند. با این حال، در ورای ظاهر بی‌ضرر آن‌ها، دامنه‌ای است مملو از خطرات و آسیب‌های احتمالی پنهان‌شده که ممکن است حریم خصوصی و امنیت کاربر را به خطر بیندازد؛ بنابراین در کنار مزایا استفاده از کوکی‌ها معایبی هم دارد.

الف. مزایای کوکی‌ها:

۱. تجربه کاربری پیشرفته: کوکی‌ها وبسایت‌ها را قادر می‌سازند تنظیمات برگزیده کاربر، مانند اعتبارنامه ورود، اولویت‌های زبان و محتویات سبد خرید را به خاطر بسپارند. این امر با حذف نیاز به واردکردن مکرر اطلاعات، راحتی کاربر را افزایش می‌دهد؛
۲. شخصی‌سازی: کوکی‌ها رفتار و اولویت‌های کاربر را دنبال می‌کنند و به وبسایت‌ها اجازه می‌دهند محتوا و توصیه‌ها را براساس علایق فردی تنظیم کنند. این باعث ایجاد یک تجربه مرور جذاب‌تر و مرتبط‌تر می‌شود؛
۳. مدیریت جلسه: کوکی‌های جلسه با حفظ اطلاعات جلسه کاربر، جابه‌جایی یکپارچه در وبسایت‌ها را تسهیل می‌کنند. آن‌ها تداوم را در چندین صفحه و تعاملات در طول یک جلسه مرور را تضمین می‌کنند؛
۴. تجزیه و تحلیل و عملکرد: کوکی‌ها در جمع‌آوری داده‌های ناشناس در مورد استفاده و عملکرد وبسایت مفیدند. این اطلاعات به صاحبان وبسایت کمک می‌کند الگوهای ترافیک را تجزیه و تحلیل کنند، محتوای محبوب را شناسایی کنند و پلتفرم‌های خود را برای تعامل بهتر کاربر بهینه کنند» (Layeeq, 2024, p. 1).

ب. معایب کوکی‌ها:

۱. نگرانی‌های مربوط به حریم خصوصی: کوکی‌ها می‌توانند اطلاعات حساس، از جمله تنظیمات برگزیده کاربر، تاریخچه مرور و داده‌های جمعیتی را ذخیره کنند. این نگرانی‌هایی را در مورد حفظ حریم خصوصی ایجاد می‌کند؛ به‌ویژه وقتی از کوکی‌ها برای ردیابی رفتار کاربر در چندین وبسایت بدون رضایت صریح استفاده می‌شود؛
۲. خطرات امنیتی: عوامل مخرب می‌توانند از آسیب‌پذیری‌های موجود در کوکی‌ها برای راه‌اندازی حملات مختلف، مانند برنامه‌نویسی بین‌سایتی، جعل درخواست بین‌سایتی^۴ و ربودن جلسه، سوءاستفاده کنند. این حملات می‌توانند حساب‌های کاربری را به خطر بیندازند، اطلاعات حساس را به سرقت ببرند و اقدامات غیرمجاز را از طرف کاربران انجام دهند؛

1. First Party cookies

2. Third Party cookies

3. <https://parspack.com/blog/programming/webserver-tutorial/what-is-cookie>. (last visited 6 May 2024)

4. cross-site request forgery (CSRF)

۳. ردیابی و پروفایل‌سازی: کوکی‌های شخص ثالث، که اغلب از طریق تبلیغ‌کنندگان و ارائه‌دهندگان تجزیه و تحلیل استفاده می‌شوند، فعالیت کاربران را در وبسایت‌های مختلف دنبال می‌کنند تا پروفایل‌های دقیقی برای تبلیغات هدفمند ایجاد کنند. این ردیابی گسترده حریم خصوصی کاربر را نقض می‌کند و نگرانی‌های اخلاقی را در مورد جمع‌آوری و نظارت بر داده‌ها ایجاد می‌کند؛

۴. چالش‌های مدیریت کوکی‌ها: با گسترش کوکی‌ها در سراسر وب، مدیریت تنظیمات کوکی‌ها و مجوزها برای کاربران پیچیده‌تر می‌شود. باوجود تنظیمات مرورگر برای کنترل رفتار کوکی‌ها، کاربران اغلب پیگیربندی مؤثر این تنظیمات را چالش‌برانگیز می‌دانند. Layeeq, 2024, p. (2)؛

۵. تأثیرات مرورگر: کوکی‌ها براساس استفاده از اینترنت محدود نمی‌شوند. هر زمان که کاربر در وب گشت‌وگذار می‌کند، کوکی‌های بیشتری جمع می‌شود؛ مگر اینکه کاربر آن‌ها را حذف کند. این کوکی‌ها بخشی از فضای هارد دیسک خواهند بود. این درنهایت باعث کندی یا تأخیر مرورگر می‌شود (Roomi, 2021, p. 2).

۴. نگرانی از نقض حریم خصوصی توسط کوکی‌ها

همان‌طور که قبلاً گفته شد، می‌توان کوکی‌ها را مسدود کرد، اما برخی از وبسایت‌ها زمانی که ما قبولشان نکنیم، مؤثر نیستند. برخی از ما صرفاً برای استفاده از وبسایت‌ها و به‌دست آوردن عملکرد کامل، کوکی‌ها را ناخواسته می‌پذیریم و البته نگران حریم خصوصی خود هستیم. ما همچنین می‌توانیم آن‌ها را پس از بستن مرورگر حذف کنیم. بااین‌حال وبسایت‌ها به‌گونه‌ای طراحی و کار می‌کنند که مسدودکردن کامل کوکی‌ها تجربه خوشایندی برای کاربران نخواهد بود. علاوه‌بر گزینه‌های ذکرشده در بالا، شخص می‌تواند از طریق یک ناشناس مرور کند، که هویتش را پنهان می‌کند. به‌هرحال کوکی‌ها هنگام مرور وبسایت‌ها تقریباً ضروری شده‌اند، اما همه ما باید درمورد این فناوری خاص به‌منزله به‌خطرانداختن حریم خصوصی شخصی که از آن استفاده می‌کند نگران باشیم (Jegatheesan, 2013, p. 2).

کوکی‌ها از طریق وبسایت‌هایی که ما بازدید می‌کنیم یا حتی گاهی اوقات از طریق وبسایت‌های شخص ثالث، که در بازاریابی و ارائه آگهی مشارکت دارند، تنظیم می‌شوند. حتی این احتمال وجود دارد کوکی‌هایی را از وبسایت‌هایی دریافت کنیم که هرگز درباره آن‌ها نشنیده‌ایم یا هرگز از آن‌ها بازدید نکرده‌ایم، اما آن وبسایت‌ها با وبسایت‌هایی که بازدید می‌کنیم مرتبط‌اند. این وبسایت‌ها فعالیت‌های مختلفی مانند تبلیغات، کمک به بازاریابی برند یا محصول، افزایش درآمد و یا حتی ردیابی کاربران را انجام می‌دهند. این وبسایت‌ها ممکن است کوکی‌هایی تنظیم کنند که قادرند حرکت کاربران را از یک وبسایت به وبسایت دیگر ردیابی کنند و داده‌های شخصی را ادغام کنند و گاهی آن را برای هرکسی که علاقه تجاری دارد در دسترس قرار دهند و اینجاست که باید نگران تجاوز به حریم خصوصی باشیم؛ چراکه کوکی‌های جمع‌آوری اطلاعات تقریباً چندان واضح نیستند^۱. مورد دیگر که می‌توان به وضعیت فوق اضافه کرد، این است که وبسایت‌ها به‌سادگی در ردیابی متوقف نمی‌شوند. آن‌ها نمایش تبلیغات را شروع می‌کنند، کمپین‌هایی در اطراف کاربر انجام می‌شود تا او را مجبور کنند چیزی را بخرد یا نگاهی به آن داشته باشد. این توانایی ما را برای جست‌وجوی چیزهای جدید از بین می‌برد. با توجه به ترجیحات کاری که قبلاً انجام داده‌ایم، همیشه همان چیزها به ما نشان داده می‌شود (Jegatheesan, 2013, p. 3). ردیابی کوکی‌ها در واقع تهدیدی برای حریم خصوصی کاربر است. از آنجاکه کوکی‌های ردیابی، داده‌های مربوط به رفتار افراد در اینترنت را جمع‌آوری می‌کنند، برای صاحبان وبسایت کاملاً ضروری است که به کاربران خود اجازه دهند بر کوکی‌هایی که رضایت می‌دهند کنترل داشته باشند. طبق مقررات عمومی حفاظت از داده‌ها (GDPR)، هر کاربر وب باید این گزینه را داشته باشد که کوکی‌ها را هنگام مرور اینترنت بپذیرد یا رد کند و اگر هر وبسایتی این گزینه را در اختیار کاربران خود قرار ندهد، مقررات عمومی حفاظت از داده‌ها را نقض می‌کند.

1. Real time Scenario from <http://www.artbusiness.com/cookies.html>

همچنین طبق مقررات عمومی حفاظت از داده‌ها، کاربران در رابطه با داده‌های شخصی خود حقوقی مانند حق دسترسی، اصلاح، محدودیت، پس‌گرفتن رضایت، اعتراض، قابلیت حمل و پاک‌کردن را دارند. همچنین حق دارند به تصمیم‌گیری خودکار و پروفایل‌سازی و پردازش داده‌های شخصی خود برای بازاریابی مستقیم اعتراض کنند (مواد ۱۵-۲۲).

نگرانی دیگری که درمورد کوکی‌ها وجود دارد مشکلات امنیتی با کوکی‌هاست؛ درحالی‌که کوکی‌ها اهداف قانونی را در عملکرد وب انجام می‌دهند، زمانی که ازطریق نهادهای مخرب دست‌کاری می‌شوند، تهدید مهمی نیز به شمار می‌روند. مهاجمان می‌توانند از تکنیک‌های مختلفی برای سوء استفاده از کوکی‌ها برای فعالیت‌های شرورانه استفاده کنند:

۱. «هایجک‌کردن جلسه^۱ با سرقت کوکی‌های جلسه: مهاجمان قادرند هویت کاربران قانونی را جعل کنند و به حساب‌های آن‌ها دسترسی غیرمجاز داشته باشند. این کار به آن‌ها امکان می‌دهد تراکنش‌های جعلی انجام دهند، داده‌های کاربران را دست‌کاری کنند و یکپارچگی پلتفرم‌های آنلاین را به خطر بیندازند؛

۲. اسکرپت بین‌سایتی^۲: اسکرپت‌های مخرب تزریق‌شده به وب‌سایت‌ها می‌توانند کوکی‌های ذخیره‌شده در مرورگرهای کاربران را دست‌کاری کنند. این کار به مهاجمان اجازه می‌دهد کد دل‌خواه را اجرا کنند، اطلاعات حساس را سرقت کنند و حملات بیشتری را علیه بازدیدکنندگان ناآگاه انجام دهند؛

۳. جعل درخواست بین‌سایتی^۳: مهاجمان قادرند از آسیب‌پذیری‌های CSRF برای دست‌کاری کوکی‌ها و اجرای اقدامات غیرمجاز از طرف کاربران احرازهویت‌شده استفاده کنند. این شامل شروع تراکنش‌های تقلبی، تغییر تنظیمات حساب یا انجام فعالیت‌های مخرب بدون رضایت کاربر است؛

۴. مسمومیت با کوکی‌ها^۴: با دست‌کاری مقادیر کوکی، مهاجمان قادرند داده‌های جلسه، تنظیمات برگزیده کاربر و توکن‌های احراز هویت را دست‌کاری کنند. این کار به آن‌ها امکان می‌دهد کنترل‌های امنیتی را دور بزنند، امتیازات را افزایش دهند و به منابع حساس دسترسی غیرمجاز پیدا کنند» (Layeeq, 2024, p. 3). در مواردی داده‌های کاربران و ارتباطات ممکن است بنا به ضرورت و به نفع امنیت ملی یا هر نگرانی مشابه دیگری استفاده شود. اما بسیاری از ما نمی‌دانیم راه‌های دیگری نیز وجود دارد که ممکن است از داده‌های ما استفاده شود.

زمانی که ازطریق پنجره‌های مرورگر خود نگاهی بیندازیم و داده‌های ضروری را درمورد کارهایی که انجام می‌دهیم، کارهایی که بیشتر وقت خود را صرف آن می‌کنیم یا آنچه دوست داریم جمع‌آوری کنیم، ما می‌خواهیم هیچ‌کس این جزئیات را نداند یا دست‌کم فکر می‌کنیم زمانی که کسی می‌خواهد این اطلاعات را برای هر نوع تجارتی یا منافع استفاده کند باید از ما اجازه بگیرد. ممکن است از داده‌های جمع‌آوری‌شده سوءاستفاده شود (Jegatheesan, 2013, p. 5). نمی‌توان هیچ‌گونه نقضی در نحوه استفاده از داده‌ها پس از جمع‌آوری با رضایت کاربر ایجاد کرد. موارد مشابهی در وب‌سایت‌های کاربایی آنلاین گزارش شده است (Vijayan, 2003, p. 10)، جایی که از این نوع داده‌ها برای اهداف بازاریابی با منافع تجاری پس از فروخته‌شدن آن‌ها به شخص ثالث استفاده می‌شود. یک کوکی می‌تواند به وب‌سایت‌ها کمک کند فروش خوبی داشته باشند یا تجارت بهتری ایجاد کنند، اما این امر به دلیل مسائل مربوط به حفظ حریم خصوصی برای کاربر چندان خوشایند نیست.

کاربردهای فعلی کوکی‌ها به ما می‌گوید که چرا کاربران باید نگران نقض حریم خصوصی خود باشند؟ همان‌طور که قبلاً ذکر شد، شرکت‌ها از تکنیک‌های مختلفی برای جمع‌آوری اطلاعات استفاده می‌کنند و سپس با اطلاعات اضافی ترکیب کرده و از اطلاعات کاربران برای هدف‌گیری رفتاری پروفایل درست می‌کنند. نویسنده چهار مسئله اخلاقی عصر اطلاعات^۵ درمورد اینکه چگونه پروفایل‌سازی حریم خصوصی را نقض

1. Session Hijacking

2. Cross-site scripting

3. Cross-Site Request Forgery (CSRF)

4. Cookie Poisoning

5. See: Mason, Richard O. Four Ethical Issues of the Information Age. Management Information Systems Quarterly. 10.1 (1986).

می‌کند صحبت می‌کند. وقتی می‌گوید: «شاید من یا شما آزادانه اطلاعاتی را دربارهٔ خودمان در هریک از پایگاه‌های داده جداگانه ارائه کرده باشیم، اما این به‌خودی‌خود به‌منزلهٔ رضایت شخصی برای ادغام و استفاده از داده‌ها نیست» (Jegatheesan, 2013, p. 5). هنگامی که کاربری در اینترنت وارد می‌شود و نام خود را ثبت می‌کند یا فرمی را به‌صورت برخط پر می‌کند در واقع پروفایلی از اطلاعات شخصی خود را در دسترس شرکت‌های گوناگون قرار می‌دهد. بسیاری از شرکت‌ها نیز با استفاده از کوکی‌ها به جمع‌آوری اطلاعات شخصی کاربران می‌پردازند.

اپراتورهای شبکه‌های اجتماعی هم با قراردادن کوکی‌ها در رایانهٔ کاربران شبکه، به ثبت صفحات مشاهده‌شده توسط کاربران، آدرس IP، موقعیت مکانی و وسایلی که از آن استفاده می‌کند می‌پردازند. درواقع شرکت‌ها از اطلاعات شخصی فقط برای ارائهٔ محصول یا خدمت استفاده نمی‌کنند. از این اطلاعات در موارد گوناگون سیاسی و اجتماعی هم بهره می‌برند (Awsat et al., 2019, p. 1354).

وبسایت‌ها و شرکت‌هایی که بازاریابی آنلاین را از طریق کوکی‌ها انجام می‌دهند باید خط‌مشی‌های شفاف داشته باشند و گزینه‌های روشنی را درمورد نحوهٔ ذخیره، استفاده یا انتقال اطلاعات شخصی به افراد ارائه دهند. این امر باعث افزایش انتخاب آگاهانهٔ کاربران درمورد رضایت آن‌ها برای هرگونه فعالیت، استفادهٔ صحیح آزادانه از فضای اینترنت می‌شود. بازبودن ممکن است به آن‌ها کمک کند تجزیه و تحلیل اطلاعاتی را، که زیربنای فعالیت آنلاین آن‌هاست و ممکن است از خدماتی که به آن‌ها تکیه می‌کنند پشتیبانی کند، درک کنند و بپذیرند. ارائهٔ انصراف‌های واضح به افراد امکان می‌دهد هنگام استفاده از سرویس‌های وب آنلاین کنترل خود را اعمال کنند. برخی افراد ممکن است بخواهند از یک وبسایت بازدید کنند، بدون این‌که هیچ سابقه‌ای از رفتار آنلاین آن‌ها حفظ شود؛ بنابراین ارائهٔ ابزاری ساده برای غیرفعال کردن هدف‌گذاری تبلیغات با استفاده از داده‌های رفتاری، امر خوبی است. این الزامی قانونی تحت قوانین حریم خصوصی و ارتباطات الکترونیکی است^۱ که به فرد بگوید چه زمانی قرار است اطلاعات روی تجهیزات ذخیره شود. برای مثال به‌شکل یک کوکی معمولی، یا کوکی فلش، و به او این فرصت^۲ را بدهد که از این کار امتناع کند. همچنین ایدهٔ خوبی است که به کاربران توصیه‌های مربوطه درمورد نحوهٔ استفاده از تنظیمات مرورگر وب خود یا انتخاب‌های ارائه‌شده در خود وبسایت داده شود و این امکان فراهم شود تا کاربر ناشناس بودن آنلاین خود را حفظ کند؛ برای مثال با اطمینان از این‌که شناسایی اطلاعات آن‌ها در پایان یک جلسه یا هر راه‌حل مشابه دیگری پاک می‌شوند.

بنابراین کاربران باید از نحوهٔ ایمن بودن حضور آنلاینشان، نحوهٔ استفاده از اطلاعاتشان و از وضعیت فعلی عملکرد کوکی‌ها و تکنیک‌های بازاریابی آنلاین آگاه شوند. به‌هرحال کاربران با مشاهدهٔ کوکی‌ها همیشه یک نگرانی و احساس ناامنی درمورد نقض حریم خصوصی و دزدیده شدن اطلاعاتشان دارند.

نتیجه‌گیری

در چشم‌انداز وسیع فناوری دیجیتال، کوکی‌ها نقشی اساسی در افزایش تجربهٔ کاربر و تسهیل تعاملات شخصی شده در وب دارند. بااین‌حال، در ورای ظاهر بی‌ضرر آن‌ها، حجم وسیعی از خطرات و آسیب‌های احتمالی همچون ردیابی و پروفایل‌سازی، چالش‌های مربوط به مدیریت کوکی‌ها و خطرات امنیتی، که می‌تواند حریم خصوصی و امنیت کاربران را به خطر بیندازد، وجود دارد.

همان‌طور که تاکنون بحث شد، در مجموع دو خطر اصلی از ناحیهٔ کوکی‌ها وجود دارد که همهٔ خطرات دیگر تحت‌تأثیر آن قرار می‌گیرند؛ یک خطر تجاوز به حریم خصوصی است و دومین خطر آسیب‌پذیری امنیتی است. کوکی‌ها می‌توانند فعالیت‌های آنلاین ما را در وبسایت‌های مختلف در طول زمان ردیابی کنند و پروفایلی از علایق و ترجیحات ما را ایجاد کنند. این اطلاعات می‌تواند توسط تبلیغ‌کنندگان برای هدف‌قراردادن ما با تبلیغات شخصی استفاده شود یا بدون رضایت ما، داده‌ها به شخص ثالث فروخته شود. این درحالی است که در چهارچوب

1. See: Privacy and Electronic Communications Regulations (PECR) <http://www.legislation.gov.uk/uksi/2003/2426/contents/made>

قوانین بین‌المللی مربوط به حفاظت از داده‌ها، استفاده از داده‌های شخصی و پردازش آن، بدون کسب رضایت صریح شخص، غیرمجاز است و در صورت کسب اجازه هم صرفاً برای هدف مورد رضایت شخص بهره‌برداری می‌شود.

در خصوص آسیب‌پذیری‌های امنیتی باید گفت در مواردی، داده‌های کاربران و ارتباطات ممکن است بنا به ضرورت و به نفع امنیت ملی یا هر نگرانی مشابه دیگری توسط دولت‌ها استفاده شود؛ اما راه‌های دیگری نیز وجود دارد که ممکن است داده‌های ما سرقت یا از آن‌ها استفاده نابه‌جا شود؛ آنجا که مجرم‌ان سایبری به نام هکر وجود دارند که می‌توانند از کوکی‌ها برای دسترسی به اطلاعات حساب ما یا سرقت داده‌های حساس از طریق فرایندی به نام اسکرپت بین‌سایتی سوءاستفاده کنند. همچنین هکرها اسکرپت‌های مخرب را به یک برنامه یا فایل قابل اعتماد مانند یک کوکی برای انجام کارهای ناخوشایند خود اجرا یا تزریق می‌کنند. در مجموع به نظر می‌رسد امکان نقض حریم خصوصی و به خطر افتادن داده‌های شخصی از طریق کوکی‌ها در مقیاس کم وجود دارد.



منابع

- انصاری، باقر (۱۳۸۳). حریم خصوصی و حمایت از آن در حقوق اسلامی تطبیقی و ایران. مجله دانشکده حقوق و علوم سیاسی دانشگاه تهران، ۶۶(۵۲۰)، ۵۱-۱.
- اوسط، امیرعلی، امام، سیدمحمد رضا و وزیری، مجید (۱۳۹۹). بررسی قوانین و ضمانت اجرای جرائم علیه حریم خصوصی کاربران فضای مجازی در ایران، جامعه‌شناسی سیاسی ایران، ۳(۴)، ۱۳۴۸-۱۳۶۳. <https://doi.org/10.30510/PSI.2021.312198.2551>
- برزودی، علیرضا (۱۴۰۳). کوکی‌ها چه هستند و چرا باید به آن‌ها اهمیت دهید؟. قابل دسترس در <https://parspack.com/blog/programming/webserver-tutorial/what-is-cookie>, 6 May 2024
- حسام، ابوالفضل و مدیو جونئی، محمد و صالح یمرلی، حسین میری (۱۴۰۰). مسئولیت مدنی پلتفرم‌های آنلاین ناشی از نقض حریم خصوصی اطلاعاتی از سوی کاربران؛ مطالعه تطبیقی در ایران، امریکا و اتحادیه اروپا، پژوهش‌های ارتباطی، ۲۸(۳)، ۶۹-۹۱. <https://doi.org/10.22082/cr.2021.530918.2202>
- ریسی دزکی، لیلا و قاسم‌زاده لیا، فلور (۱۳۹۹). چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر. دادگستری، ۸۴(۱۱۰)، ۱۲۳-۱۴۶. <https://doi.org/10.22106/jlj.2020.88629.2213>
- شهبازی، آرامش و شبانی کلاهی، ساناز (۱۴۰۳). چالش‌های حقوقی حفظ حریم خصوصی در شهرهای هوشمند با نگاهی به حقوق بین‌الملل و حقوق ایران. حقوق فناوری‌های نوین، ۵(۹)، ۲۲۱-۲۳۴. <https://doi.org/10.22133/MTLJ.2024.407318.1226>
- قناد، فاطمه و علیقلی، امیره (۱۳۹۹). مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی، حقوق قراردادها و فناوری‌های نوین. ۱۱(۱)، ۲۹۷-۳۲۲. <https://doi.org/10.22133/CLJ.2020.243290.1016>
- فتحی، یونس و شاهمرادی، خیراله (۱۳۹۶). گستره و قلمرو حریم خصوصی در فضای مجازی. دادگستری، ۸۱(۹۹)، ۲۲۹-۲۵۲. <https://doi.org/10.22106/jlj.2017.29234>
- مسعودی، امیدعلی (۱۳۹۹). حق کاربران بر نظارت الکترونی و حفظ حریم خصوصی در جامعه اطلاعاتی. مطالعات رسانه‌ای، ۵(۳)، ۷-۱۹.
- مقامی، امیر و عطاران، نادیا (۱۳۹۸). موازنه افشای حریم خصوصی خانوادگی چهره‌های مشهور در رسانه‌ها و آزادی بیان در رویه نهادهای قضایی. مطالعات حقوق عمومی، ۹۴(۲)، ۳۱۱-۳۳۱. <https://doi.org/10.22059/jpls.2018.219954.1390>
- یوسف‌نژاد، مسعود و طاهران‌پور، ملیکا (۱۴۰۱). کوکی در مرورگر چیست و چه اهمیتی دارد؟. قابل دسترس در سایت: <https://www.zoomit.ir/howto/132944-what-is-cookie-internet/1401/08/03>
- نکونام، وحید (۱۴۰۳). بایسته‌های تحقیق از حریم خصوصی داده‌های ارتباطاتی و اطلاعاتی در فضای سایبر. حقوق فناوری‌های نوین، ۵(۹)، ۲۷-۴۰. <https://doi.org/10.22133/MTLJ.2023.390545.1188>
- انصاری، باقر (۱۴۰۱). حقوق رسانه. تهران: سمت.
- هاشمی، سیدمحمد (۱۴۰۲). حقوق اساسی جمهوری اسلامی ایران (ج ۲)، تهران: نشر میزان.
- Singh, A. R. (2022). Right to privacy in cyberspace. *Cyber Law Reporter*, 1(1). Pp.23-34. Available at: <https://cylr.thelawbrigade.com/wp-content/uploads/sites/28/2022/11/Amisha-Rerru-Singh.pdf>
- Tripathi, K. (2020). Protection of privacy in cyberspace: A comparative analysis between India and USA. available at: <https://ssrn.com/abstract=3611622>

- Layeeq, A. (2024). Understanding Cookies: Pros and Cons in Browser Security. Available at <https://www.linkedin.com/pulse/understanding-cookies>, 6 march 2024.
- Mason, R. O. (2017). Four Ethical Issues of the Information. *Computer Ethics*.
- Peng, W., & Cigna, J. (2000). HTTP cookies—a promising technology. *Online Information Review*, 24(2), 150-153. <https://doi.org/10.1108/14684520010330346>
- Roomi, M. (2021). Advantages and disadvantages of cookies: Limitations & benefits of cookies on websites. Available at <https://www.hitechwhizz.com/2021/02/6-advantages-and-disadvantages-drawbacks-benefits-of-cookies.html>
- Jegatheesan, S. (2013). Cookies – Invading Our Privacy for Marketing, Advertising and Security Issues, *International Journal of Scientific and Engineering Research*, 4(5), 1-8. <https://doi.org/10.48550/arXiv.1305.2306>
- Vijayan, J. (2003). Users of online job services risk lack of privacy protection. *Computerworld*, 10, 5-15.

[In Persian]

- Ansari. B, (2004), Privacy and its protection in Islamic comparative law and Iran. *Journal of Faculty of Law and Political Science*, University of Tehran. 66(520), 1-51.
- Ansari, Baqer (1401). *Media Law*. Tehran: Samt.
- awsat, A. , Emam, S. M. R. and vaziri, M. (2021). Laws and Guarantees for the Implementation of Crimes in the Field of Privacy in Cyberspace in Iran. *Political Sociology of Iran*, 3(4), 1348-1363. <https://doi.org/10.30510/PSI.2021.312198.2551>
- Barzoudi. A, (2024). What are cookies and why should you care about them?, available at <https://parspack.com/blog/programming/webserver-tutorial/what-is-cookie>. May 6, 2024.
- Fathi. Y and K. Shahmoradi, (2017). the Scope of privacy in cyber space. *Judiciary Legal Journal*, 81(92) 229-252. <https://doi.org/10.22106/jlj.2017.29234>
- Hessam. A., Modibo Joni, M., Miri, H., & Yamrali, S. (2021). *the Civil liability of online platforms caused by the violation of information privacy by users; A comparative study in Iran, America and the European Union*, *Communication Research Quarterly*, 28(3), 69-91. <https://doi.org/10.22082/cr.2021.530918.2202>
- Hashemi. S. M. (2023), *Constitutional Law of the Islamic Republic of Iran (2)*. Tehran, Mizan Publications.
- Masoudi, O. A. (2019). Users' right to electronic surveillance and privacy in the information society. *Media Studies*, 15(3), 7-19.

- Maghami, Amir and Attaran, Nadia (2019). Balancing the Disclosure of Family Privacy of Famous Figures in the Media and Freedom of Expression in the Procedure of Judicial Institutions. *Public Law Studies*, 94(2), 311-331. <https://doi.org/10.22059/jpls.2018.219954.1390>
- Nekonam. V., (2024), Research requirements of the privacy of communication data and information in the cyber space. *Modern Technologies Law*, 5(9), 27-40. <https://doi.org/10.22133/MTLJ.2023.390545.1188>
- Ghanad, F. and Aligholi, A. (2020). The Notion and Importance of Personal Data and Privacy and Their Various Protections in Cyber Space. *ModernTechnologies Law*, 1(1), 297-322. <https://doi.org/10.22133/clj.2020.243290.1016>
- Raeesi Dezaki. L., & Ghasemzadeh Liasi, F. (2019). Challenges of Iran's Legal System in Violation of Personal Data and Privacy in Cyber Space. *Legal Journal of Justice*, 2084(110), 123-146. <https://doi.org/10.22106/jlj.2020.88629.2213>
- Shahbazi. A., & Shabani Kolahi, S. (2024). Legal challenges of preserving privacy in smart cities with a view to international law and Iranian law, *ModernTechnologies Law*, 5(9), 221-234. <https://doi.org/10.22133/MTLJ.2024.407318.1226>
- Youssef Nejad. M., & Taheranpour, M. (2022), What is a cookie in the browser and what is its importance?, available on at: <https://www.zoomit.ir/howto/132944-what-is-cookie-internet/2022/10/25>

COPYRIGHTS

©2025 by the authors. Published by University of Science and Culture. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0/>

