

## POLICY CONCERNING THE HTTP COOKIES

*The intensive expansion of the digital economy poses new challenges to the regulatory framework and corporate privacy policies for individuals. The enforcement of the EU's General Data Protection Regulation is triggering a new approach to the scope of personal data and the rules for their administration. There is a need for a complete reorganization of the ways in which websites study the behaviour and characteristics of online content users, which determines a change of the cookie policy out of the hidden internet area towards an unconditional need for explicit consent to their use for whatever purposes.*

*This work provides theoretical basics about the nature and variety of HTTP cookies as a web tool. It outlines what changes result from the introduction of regulatory instruments and corporate policies for the protection and administration of the personal data of individuals in real and electronic environments. On this basis, the use of cookies in modern webpages and sites has been explored, which serves to implement varied changes in the proposed internet content to achieve conversion and the resulting economic and social effects.*

*JEL: L86; K00; K19; K39*

### Introduction

The entry into force on 25 May 2018 of the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016), imposes a series of new rules for the protection of personal information which can identify each person as a consumer and customer. Mandatory implementation of the regulation sets out a number of new obligations for business, related to the responsible collection and processing of personal data, regardless of where it takes place inside or outside the Union. In the modern digital age, each internet user visits multiple web pages or sites on the global network, where significant information is transferred between the web server and the internet browser used for web content view. One part of the exchanged packages is related to the use of “HTTP Cookies” or only “Cookies”. They are a tool for collecting accurate user information without affecting the user's internet experience, as it takes place in a

---

<sup>1</sup> Assoc. Prof. Dr. Michal Stojanov is from University of Economics – Varna.

conditionally hidden process that occurs while browsing and studying a website. Their existence, application and functionality ensure electronic content providers with specific consumer information that can enhance the efficiency and precision of the digital relationship. However “the development and deployment of cookies technology in the last ... years has been the most significant – and most controversial” (Peters, 1999, p. 275) phenomenon. It is related to the business ethics of the application of cookies, the level of their aggression, which is an expression of a loyalty policy to consumers, in addition, it may be in the relationship and exchange of information with the consumer data market and the possibilities for their use by third parties for a variety of objectives.

The purpose of this work is to systematize the essence of cookies as a modern tool for collecting information about end-user work in an internet environment.

In this study, the terms website and webpage are used with a high degree of conditionality as very close concepts, despite the difference between them. The most common design of a website is a collection of webpages that are addressed by a single domain. Technically, at any point in its online experience, the user views the content of a web page, even though he/she can visit a website.

A further limitation of the conducted survey is the use of secondary statistical information by Q-Success DI Gelbmann GmbH (W3Techs), which is collected and processed according to a specific company methodology and automated algorithm and can be accomplished with certain conditionality and constraints related to representativeness of the data that the company defines as “include only the top 10 million websites (top 1 million before June 2013) in the statistics... they serve our purpose of providing a representative sample of established sites very well” (W3Techs, 2018).

In its legal definition, personal data is any information about the physical person that allows his/her individualization and clear distinction as identity. In its most recent definition, GDPR also allows personal data to be expressed using online identifiers. This extension of scope is a logical and quite natural product of tangible social development driven by the evolution and importance of information and communication technologies for contemporary public and private life. Therefore, the use of cookies today requires the user's explicit consent to the use of information society products in an electronic internet environment as it may be directly or indirectly linked to the processing of personal data of the physical entity. In this way, part of the internet experience may be accompanied by the invisible process of exchanging personal data and is therefore currently covered by a specific regulatory framework and administrative treatment regime.

### **HTTP Cookies: Theoretical Background**

In their programmable nature, cookies are a minimal component or message that is applied through the HyperText Transfer Protocol (HTTP) and is set by a specific code or programming language. They are defined as “a small piece of information implanted into the HTTP content by the server and used to identify the client on all future visits to the site” (Matthew, Goldie, 2004, p. 127). They exist in the form of a name-value pair that the web

server sends to the internet content viewer. This name-value pair is stored locally and can be saved within a specified or unlimited time as a text file. The specific information accumulated by the browser, including personal data, is sent back to the server at each subsequent visit by the user or within a continuous retrieval of information within a time-limited active session or when contacting the website or page. It follows that its functions can be fulfilled within each subsequent visit, and even within the scope of a longer web browsing or advanced information and communication exchange before the waiting time of the session expires. The information collected and formatted is in the form of a “file through which the user is identified, and thus repeat visits are not counted” (Salova 2014, p. 43), this means that the cookie is a tool for conditional reporting and differentiation of unique from loyal visitors. With regard to the security of online user sessions, it should be kept in mind that cookies do not appear in their pure form as malware, they are not related to automatic execution of commands to manipulate the browser, other programs or the operating system used or other atypical behaviour of computer systems. Cookies play the role of “verification sent back to the programmer that a piece of software code is running smoothly, and that entire process is worthwhile” (Hannaham 1996). However, the specificity of the internet technology, which implies that the participants in the information process are conditionally identified as senders and recipients of digital packets, means that any intermediate and terminal device in the communication process can be relatively accurately identified and thus a seemingly impersonal information is associated with another that is inherently personal data, such as a user IP address. In this way, cookies that are designed to perform a basic information function are a powerful tool through which digital companies can get specific data about their users. Sometimes this data may not have a standalone and direct application but, in combination with other information, it is an effective mechanism for impact and a way to anticipate consumer expectations or to purposefully attempt to stimulate consumer responses. Fields that define the syntax of a cookie may contain different attributes: the activity period, which may be, for example, until the end of the current session or closure of the internet content browser; the domain name, and the internet path that sent the cookie; various settings for restrictions on the recipient of the information gathered. The latter is linked to the possibility that information can be identified and received by a third party, which is again determined by the cookie policy of the internet sites.

One of the main purposes of getting information about the online internet content recipients behaviour when visiting a site is within the current session or on a future visit to that internet address to have a higher level of personalized content tailored to its current or past behaviour and registered activity and responses to a particular internet matter. The information, gathered by many users aggregates to a certain extent, allowing web managers to constantly improve their content and functionality in response to real and active users' reactions and profiling them in homogeneous groups, and even the possibility of highly personalized approach.

The use of cookies in one of the most popular internet applications the browser is related to the ability of a once visited website to recognize its users in a subsequent contact. This means that the user demonstrates interest in the collection of elements on the relevant web page. This is related to the desire to improve the ability of the content provider to manipulate the information sent to respond more fully to user decisions established in

previous contacts. Thus, using the collected data for the user, it is possible to optimize the scope of the presented digital information, taking into account its individual features and preferences. Here, the degree of presentation of personalized digital material should not be absolutized because it is generally designed for certain homogeneous groups of users who exhibit similar or very close behavioural profiles in an internet environment. However, the automation of this process provides an opportunity for these alternatives to be relatively high. Of course, depending on the site's functionality and the security level of the session, customization can also be done on an individual level, such as e-banking, e-mail, virtual commerce, etc. What's more, cookies are a solution through which websites can accurately determine how many actual users were their visitors and what their behaviour was in information dimensions to which we have an economic or other interest. Such a conditional application is implemented by generating a unique user number that is part of the newly created cookie (Brain, 2000) and stored locally at the users' device, serving to distinguish new visitors from those who reached the website earlier. However, this possibility should not be perceived without certain limitations and disadvantages, as cookies cannot distinguish different users accessing a shared computer system. This disadvantage may be conditionally overcome by using individual user accounts to access information on a site, but it is also not a guarantee that the person who is currently viewing certain internet content is the account holder. Again, the latter constraint can be overcome with technologies to recognize the physiological specifics of the individual. Thus, through biometrics (a mathematical approach to recognition through the unique dimensions of the physiology of an individual via dactyloscopy, facial recognition, etc.), it is possible in real time to recognize personality, which again involves sharing a considerable amount of information about the individual and its application for safe identification. Under certain conditions, such an approach is achievable in personal smart devices (smartphones, smart accessories, etc.), where the use of certain features and applications is tied to activating a user account and sharing certain information as personal data, but this is not entirely a secure approach to ensuring credibility and absolute user authentication. Consequently, the ability to identify user behaviour of a specific person by using cookies can not be accepted or presented unconditionally. Additionally, users can change their program settings in the functionalities of today's browsers and Internet content viewers and refuse to accept and / or store cookies, but cookies still remain a "good enough indicator of how many visitors are different" (Salova, 2014, p. 43) or the same. Information related to cookies should not be accepted unconditionally because it provides relatively accurate but not completely reliable information about end-users and their information consumption. However, "cookies can be understood as a database of personal demographic, psychographic, and behavioural information, or as a temporary device for creating a stateful, tailored online environment" (Peters, 1999, p. 277). The main problem that the internet community can not promote and adopt correctly is that cookies are a tool through which "the web, and all the convenience it brings, funds itself" (Shields, 2013). Therefore, cookie technology allows companies offering a variety of conditionally free internet content and pursuing multiple economic and social goals to reach a certain desired consumer information without making resource allocation in costly and time-consuming traditional marketing research. Separately, even if the user refuses to accept or store cookies, there are other tools to help collect end-user information in an online environment. In this regard, it should be taken into account that users can anonymize their online behaviour and remain relatively invisible on the Internet

through VPN (Virtual Private Networks), proxy servers, Tor protocol and other means. This should not be accepted unconditionally, since according to Art. 251b of the Bulgarian Electronic Communications Act (Bulgarian Electronic Communications Act, 2001) entities providing public electronic communications networks and/or services shall keep data created or processed in the course of their activity for a period of 6 months. Such a solution seeks safeguards related to the needs of national security and the prevention, detection and investigation of serious crimes. The organization of the processing and storage of traffic data must be coordinated and in full compliance with the provisions of the personal data protection regime. This means that it can not be used against the general interests of consumers and for sanctioning the behaviour allowed by the regulatory framework for economic agents in an electronic environment.

Web pages and sites use a variety of internet technologies, such as cookies, which can target the following possible impacts on users that determine their types:

- Permanent and temporary cookies. The name itself indicates what period the cookies sent by the web server are stored locally on a personal device. In the case of temporary cookies, after the current session expires and the internet browser closes, they are automatically deleted. Identifying a cookie as permanent is not related to its endless storage on the user's computer. First, cookies can be removed by the user by changing the browser settings or using specialized software for this purpose. Secondly, despite their provisional designation as long-term or permanent, they have a certain storage period, which may be one or even two calendar years. It should be made clear that every subsequent visit to the same website, the latter has the ability to manipulate the remaining cookies and change their behaviour as required by the site administrator. This determines the tracking nature of permanent cookies.
- Mandatory and session cookies. Mandatory cookies should be accepted by users and their devices in order for the web page/site to function in its full capabilities and content. If they are denied, then it is possible that all of the information on the web page may not be displayed or certain items may be unavailable or inactive. However, sites are required to notify users of this type of cookie and the cookie policy they apply. Also, identifying a cookie as inherently necessary depends entirely on the owners and developers of the website. Session cookies have a “life” until the end of browsing, which may either mean leaving the page or closing the Internet browser program.
- Identifying and anonymous cookies. The first type performs the role of registering a user on a site to allow him/her to view a variety of content without having to re-authenticate each subsequent page, meaning that the web server automatically recognizes the user by the cookie-associated unique user number. This defines cookies as “an internet user ID card that tells the site when the user has returned” (Pinsent Masons LLP, 2018). Anonymous cookies collect information regardless of the strategy to identify the uniqueness of the user, but rather perceive her/him as a typical user of the website. Therefore, they quantify and specify not so much the user as the way the website is used, its efficiency and working capacity.

- Own cookies and third-party cookies. The difference between them is according to the source of the cookie, when the first one is created, it accumulates information and is sent by the site being visited, while the latter is developed by specialized companies that deal with internet audiences research and subsequent supply of high profiled content. The use of third-party cookies is done on a contractual basis and should only be for the purpose of upgrading and manipulating online content, while ensuring the protection of data confidentiality and its use. Agreeing on the use of foreign cookies implies that conditions should also be set for the dissemination of the information gathered to subsequent participants. To that end, it is possible to use appropriate standards to ensure the protection and access to information gathered by end-users of web content. It is assumed that third-party cookies are “more aggressive cookies” (SuperHosting.BG, 2017), as their application goes beyond the interests of the particular site and is expanded to perform tasks related to comprehensive promotional strategies and diverse economic and social goals of third parties.
- Targeting and advertising cookies are tailored to the behaviour of the web visitor. They serve to evaluate the effectiveness of the internet advertising used. This allows the concept of interest-based advertising to be realized so that internet users can be offered content that is fully compliant with the established online behaviour. In the internet it has been an established practice that this kind of cookies should be owned by third parties who control their content. Behind the information gathered through this type of business, there are serious economic opportunities that allow this kind of cookies and the data gathered through them to form a digital market for their exchange.

The listed criteria allow us to accept the distinction made by the International Chamber of Commerce of the UK in four main categories (ICC UK, 2012): strictly necessary, to measure efficiency, related to functionality and advertising cookies. To accomplish multiple tasks, a more complex approach is applied at the same time, in which the strict boundaries between the different categories overlap and they lose their own outline and one-dimensional application.

In this way, cookies can serve one or more of the following:

- preferred web content by the user as sections and headings visited on a website or internet;
- time spent on staying on a web page and visualizing specific web content;
- advertising messages that were on the visible part of the web page and the reactions they caused;
- cooperative affiliate programs to track user activity and cross profiling across multiple conditionally independent sites;
- a tool for a variety of marketing purposes, including an assessment of the effectiveness of sales promotion tools;

- collecting statistical information about the functioning of the site or the web page, resources used, mechanism for recording and reporting errors in the visualization of the content and the work of the site, etc.

### **New Dimensions of Protection of Personal Data**

In their genesis, cookies have been created as a means by which companies can get information about their users without distracting their presence in online space and engaging time resource for that. Running them in the background in a web browsing application renders them inconspicuous for internet users who focus their attention entirely on the web content. However, their specificity, linking keywords, actions and demonstrated interests to a user, identified as an internet address, a computer, and a web browser, creates new dimensions of the need for an adequate management of user's personal data by each administrator and any person with access to cookies. This at least means that internet users should be fully informed of the extracted cookies and their possible use and on the basis of their informed acceptance or denial of their storage and use of the information gathered through them, and further use by third parties.

The legal framework regulating the use of cookies within the EU was originally laid down in Directive 2002/58/EC (Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No 2006/2004 2009) and useful means of facilitating the provision of information society services, for example in analyses improving the efficiency of website design and advertising and checking the identity of the user engaged in online transactions. The main philosophy behind the regulatory framework is the fundamental need for users of electronic communications services over the Internet to obtain clear and comprehensive information when conducting an activity that could result in storing or gaining access to the processing of personal data and the free movement of such data. The primary consideration is related to the need in the new digital realities to ensure the right balance and effective protection of personal data and the privacy of individuals. On the one hand, the normal and seamless use of information society products must be ensured, but on the other, it must provide safety for consumers in the context of the administration of their personal data. The retention of traffic data by operators or intermediaries of the communication process is not tied to commitments to their observation or study. The imposition of liability on providers of information society communication services with regard to the lawfulness of data is a matter of national law and therefore, they must apply the principle of technological neutrality.

Obtaining consent to the processing of personal data is not an imperative action. The GDPR decides that once a person has given or refused to give his or her personal data, he or she should have the right to change this decision and to cancel it. The most important dimension of this is the ability to “be forgotten”, that is, by his own will, to prohibit the subsequent processing of his data and to have the unlimited right to request collected personal data to be removed, provided it was already used for certain purposes and in accordance with the exceptions to the Regulation. The main reason for this is the constant

change in consumer preferences and the risks that accompany this process. This means that when a person has been a customer or user of a particular real or electronic trader and has provided him with certain personal data after a change in his behaviour, he has the right to request that these data be removed from the administrator's registers. Possible exceptions to this principle are related to reasons of public interest where the preservation of this personal data may have applications in the field of history, health, statistical purposes or future legal claims related to that information. At this stage, a clear and specific definition of the lawful use of collected information in the form of personal data has a comprehensive regime and is extremely important in terms of equality and the universality of treatment.

Although the cookie has been created as an automated user feedback tool to diagnose and collect feedback on the website, it quickly acquires the functions of an instrument of outstanding economic and social significance. This transformation brings us to the point where, in terms of the privacy policy the cookie can be defined as a medium or tool that provides wide scope for identifying the user within the meaning of the definition of personal data. This requires the internet user to give his explicit consent regarding the acceptance of cookies and their use for marketing and other purposes. Thus, personal and non-personal information exchanged can be used for a variety of business and other purposes by the site owner, the cookie creator, and/or third parties.

Furthermore, with the introduction of the GDPR, the application of the collected information from an organization can not be directly transferred to a third party unless explicit consent is given. This means that end-users are entitled to take a position on such use of their data for a wide range of economic and other impacts from third parties that, by commercial or alternative means, have obtained information about them. The behaviour and actions of participants in a situation where a person has given his permission to use his personal data, subsequently transferred to a third party, but in the meantime, the person has decided to change his original position and refuses to the first party to process more of his data and may even take advantage of the right to be forgotten. In such a situation, it is possible to assume that the original consignee, as initiator and executor of the transmission of the information to a third party, assumes responsibility for informing the addressee of the change in the initial administration consent situation. This is linked to the resulting possibilities for the third party to be penalized for its bad conduct, in identifying the unallowed and unauthorized use of personal data that has been denied to the user for a higher-level right of use.

Also, one of the benefits of cookies is that as a web tool, they act as a hidden element of the website or page and are most often written in a specialized programming language. Exploring the settings of the internet content browsing program used, the user could review and explore the cookies received in general. This allows the program administrator to remove the stored information on the local device, including stored cookies. The latter means that its information records can be locally deleted, by applying this mechanism, the system is brought to its original state, which means that it is ready to exchange information. In this way, the relative restart will re-initiate a process for accepting cookie policies on the visited websites or pages. Such a process of resetting to default can be perceived as a working technological solution to the "right to be forgotten".

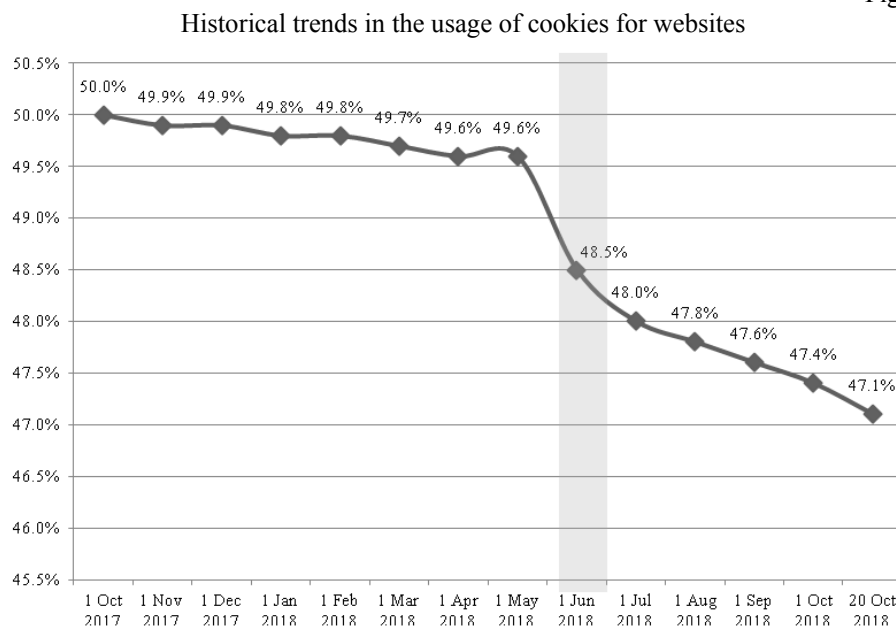


The imposed changes to the privacy policy require the cookie application to be implemented after a request for their management is received, and only after a clear consent from the person whose data will be used, which can also be done electronically. An electronic statement of intent must be digitally documented and stored in an appropriate manner, this may also be done under a regime in which the written form is deemed to be complied with if an electronic document containing an electronic statement is present (Bulgarian Law on Electronic Document and Electronic Signature, 2007).

### Usage of Cookies

According to the W3Techs technology company, within the scope of a systematic global survey as of 27.07.2018, 47.8% of all websites use cookies (W3Techs, 2018). This indicates the importance of this web tool and its popularity in the global network. It is important to note that within the one-year observation of the use of various elements included in websites, a slight downward trend of development is formed. The reduction in the use of cookies is further influenced by the entry into force of the GDPR principles and rules by the end of May 2018. A decline of 1.1% unlocks a process of rethinking the use of cookies from websites. Extending the scope of the definition of personal data leads to the denial of excessive use of cookies, and currently less than half of the sites use this web tool (see Figure 1). The 2.6% cookie reduction for the 12-month period from 01.10.2017 to 01.10.2018 is also an expression of the strategy for using alternative means of collecting and using the information to personalize the services provided to end-users, forming the modern information society.

Figure 1



Source: W3Techs 2018.

It is necessary to assume that the downward trend in the use of website cookies is a legitimate response to technological changes whereby electronic traders, by outsourcing the creation and service of the online digital exchange platforms used, take advantage of the benefits to get ready-made e-commerce software solutions. The latter integrates third-party consumer information, meaning that the website does not have to collect information that is accumulated and processed at a higher and specialized level on the internet and can be applied as a finished product in the form of a set of data. In this way, the collection and processing of user information as a function and activity are entrusted to a third party, which is producing reports on the served user segments and website visits, which can be dynamic and updated as information content in real time. The detailed statistics allow us to study in a great depth the aspects related to: the functioning of the site and the visualization of its information in the internet environment, search engine indexing, traffic sources, internet commerce conversions, follow-up of the marketing campaigns, user flow visualization, and a host of other metrics, tables, infographics, automatic messages, alarms, etc. (WEBSITE BG, 2012). In addition, through the use of an external contractor, who is responsible for the presentation of a company on the web, allows the agents of commercial exchange to concentrate on those elements and activities in which they are the best and competent, namely the divestiture and management of processes related to it. Thus, for all other service tasks, a dedicated agent is engaged, whose loyalty and responsibility is a factor for the success of any business initiative in an electronic environment. Moreover, the transfer of performance towards an external organization transfers to it the responsibilities related to the management of personal information concerning the users. This means that any weaknesses and omissions that may cause violations of laws and regulations in the field of personal data protection, the rights of individuals and third parties in connection with the administration of such information as well as the possible violations and the ensuing of sanctions from control authorities can be contractually transferred as a liability to the outside contractor. This is also admissible under Art. 37 GDPR, where the Data Protection official can perform its functions on the basis of a service contract (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC 2016).

The fact that only half of the websites covered by W3Techs are using cookies may be due to the circumstance that part of them in their content is digital business cards of certain economic or social entities or individuals who in their digital strategy do not seek to use the internet as an economic activity environment or study of online audiences but rather as a platform for their presentation to a wider virtual audience. In this situation, the Internet is used only as an electronic channel for informing potential customer segments.

The use of cookies as a tool for registering user activity continues to be an essential element of modern websites but in a new mode of more responsible and committed behaviour of recipients of this information. The latter is an expression of the growing need for trust and loyalty of the processes taking place in a digital environment. This requires a higher level of responsibility and commitment of web content administrators to end-users receiving and managing personal data. Last but not least, the applicable consent or waiver regime with regard to the management of personal data must be customized in such a way as to make it as easy as possible and without misleading the interests of end-users of internet content.

## **Conclusion**

Used for the purposes of recognizing or collecting user-related statistics, cookies are a popular tool used on the internet. Modern digital society sets new higher requirements for the development of adequate and comprehensive digital content delivery policies that all online players have to take into account. The main direction of the cookie application as an automated web tool should be to achieve higher levels of personalization of the offered internet content, awareness and optimal protection of user data.

Several major issues have been raised in the development of the essence, varieties and state of the cookie application embedded in and functioning on modern websites and web pages. The most important points are:

1. Cookies are a web technology for automated data exchange between the server and the end-user internet content viewer. They can be clearly divided into several kinds, but the specificity and necessity of complexity of the information collected implies their simultaneous application.
2. In the course of the analysis, it was found that there was a general reduction in the use of web-based HTTP cookies, which is a legitimate response to the introduction of the stricter and comprehensive General Data Protection Regulation – GDPR, which has been in operation since late May 2018 and includes online identifiers, such as the end user's IP address, within the scope of protection.
3. By appropriately modifying the cookie policies of websites and webpages, subject to explicit permission from the physical person, HTTP cookies may be installed on the user's local device and certain data about his internet behaviour and for the effectiveness of the functioning of the website or web page, which consent can be unlimitedly changed over time.

The chosen theme for examining the application of HTTP cookies to obtain specific consumer information that can be applied to individualize the Internet content offered has its economic and social significance and identifies opportunities for future research in this regard.

Changes in the regulatory framework for personal data protection mean that special attention should also be paid to online identifiers. This will allow for greater protection of personal data and balance of the interests of members of the information society. In this context, cookie policies should reflect new regulatory realities and offer adequate information security to affected parties.

## **References**

- Brain, M. (2000). How Internet Cookies Work, viewed 27 July 2018, <https://computer.howstuffworks.com/cookie.htm>.
- Bulgarian Electronic Communications Act. (2001). viewed 10 November 2018, <https://www.lex.bg/laws/ldoc/2135180800>.

- Bulgarian Law on Electronic Document and Electronic Signature. (2007). viewed 4 November 2018, <https://lex.bg/laws/ldoc/2135553187>.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector' 2002, Official Journal of the European Union, L 201/37, vol 036, no. 32002L0058, pp. 63-73, viewed 11 Ноември 2018, <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:32002L0058&from=BG>.
- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws' 2009, Official Journal of the European Union, vol L 337, no. 32009L0136, pp. 11-36, viewed 11 Ноември 2018, <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=OJ:L:2009:337:FULL&from=BG>.
- Hannaham, J. (1996). Microchips Ahoy! New Advertisers Track Your Crumbs. – Village Voice, 20 August 1996.
- ICC UK. (2012). ICC UK Cookie Guide', Edition 2, International Chamber of Commerce United Kingdom, London.
- Matthew, S., Goldie, P. (2004). Optimizing Network Performance with Content Switching: Server, Firewall, and Cache Load Balancing. Prentice Hall Professional, New Jersey.
- Net Info AD. (2015). Cookie policy, Sofia, Bulgaria, viewed 28 June 2018, <https://passport.netinfo.bg/nipass/index.php?cmd=termscookie>.
- Net Info AD. (2018). Privacy policy, София, България, viewed 28 June 2018, <https://www.netinfocompany.bg/privacy.php>.
- Official Journal of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC', 4 May 2016, pp. 1-88, viewed 20 July 2018, <https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=BG>.
- Peters, T. A. (1999). Computerized Monitoring and Online Privacy. McFarland & Company, Inc., Publishers, Jefferson.
- Pinsent Masons, LLP. (2018). Cookies: Frequently Asked Questions, viewed 31 July 2018, <https://www.aboutcookies.org/cookie-faq/>.
- Salova, S. (2014). Evaluation of e-commerce websites on the basis of usability data. – Izvestiya (academic scientific journal of the University of Economics – Varna), Vol 3, pp. 38-49.
- Shields, R. (2013). Trust is the best alternative to cookies. – Marketing Week (Online Edition), 8 September 2013. Viewed 29 October 2018, <http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=90425821&site=ehost-live>.
- SuperHosting.BG. (2017). Session (temporary) and permanent HTTP cookies (HTTP cookies), viewed 27 July 2018, <https://help.superhosting.bg/session-cookies-and-persistent-cookies.html>.
- W3Techs. (2018). Historical trends in the usage of site elements for websites. Viewed 20 October 2018, [https://w3techs.com/technologies/history\\_overview/site\\_element/all](https://w3techs.com/technologies/history_overview/site_element/all).
- W3Techs. (2018). Technologies Overview. Viewed 4 November 2018, <https://w3techs.com/technologies>.
- W3Techs. (2018). Usage of Cookies for websites. Viewed 27 July 2018, <https://w3techs.com/technologies/details/ce-cookies/all/all>.
- WEBSITE BG. (2012). 11 tricks with Google Analytics for your site – Part 1 and Part. Viewed 10 November 2018, <https://www.website.bg/public/articles/itemId/165> и <https://website.bg/public/articles/itemId/169>.