International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 4S, 2025
https://www.theaspd.com/ijes.php

Consent to Processing Personal Data in Online Behavioral Advertising as Per the GPDR and Experience for Vietnam

Dr. Vo Trung Hau
Binh Duong University, Vietnam
vthau@bdu.edu.vn

Abstract: Computers leave life and turn personal information into a valuable asset that can influence the treatment reason for personal data. Online behavioral advertising aims to match advertising to Internet users by applying personal data processing procedures that may result in the control of human behavior. Tracking technologies such as Web cookies, cookie walls, hidden cookies, web beacons, and device fingerprints violate the rights of private Privacy, one's information, and the rights of one's owner. EU law provides data about the reason for consent, whether personal data in advertisement fox direct behavior line Right give go out one way free, knowledgeable, specific, clear. The article analyzes the provisions of Vietnamese law on online behavioral advertising and provides recommendations for improvement.

Keywords: Online behavioral advertising; consent reason data; personal information

1. INTRODUCTION TO THE PROCESSING OF PERSONAL DATA FOR ONLINE BEHAVIORAL ADVERTISING

1.1. Overview of personal data processing

The advent of computers has played a significant role in transforming personal information into a valuable asset and has significantly impacted the collection of personal information. Computers can store large amounts of information in raw data relatively quickly, cheaply, and virtually indefinitely at incredible speeds. The result of processing is often the creation of new information that serves as the basis for human or computer decision-making. The development of telecommunications technology with the connection of computers to the Internet, allowing the transmission of information between computer systems, has made information increasingly important and promoted the collection and use of personal information. All personal information can be shared by different computer users on the network. Some risks associated with using computers to process personal information include data being accessed or disclosed inaccurately, incompletely, or used for purposes other than those for which the information was collected. A person's home, finances, mental state, physical condition, and thinking can be exposed to the most casual observer. Financial institutions collect and provide information on people's creditworthiness and drinking habits, health, characteristics, reputation, extramarital relationships, religious beliefs, criminal records, race, sexual preferences, etc. As a result, financial institutions can reveal a complete profile of a person's ability to repay a loan and his or her entire personal life. In addition, direct marketing agencies profile individuals for online behavioral advertising. The term data protection comes from the German term "Datenschutz." According to Bennett, "*data protection*" is a technical term that refers to "*a set of policies enacted to regulate the collection, storage, use, and transmission of personal information*. "Hondius describes data protection as "*the body of law that guarantees to every individual, regardless of nationality or place of residence, respect for fundamental freedoms and in particular the right to Privacy, about the automated processing of personal data*." Bygrave defines personal data protection as a set of measures, a set of data processing principles, aimed at protecting people from harm caused by processing their personal information. According to the European Commission's classification personal data is divided into: (i) contact information such as home address, place of work of the individual, email address, telephone number; (ii) technical data such as IP address, device-related data on type, international mobile equipment identity (IMEI), browser information; (iii) demographic data such as age, ethnicity, gender, education level, occupation, household income, number, gender, age of household members; (iv) location data such as mobile

device, GPS data and travel history entered into satellite positioning system, radio frequency identification (RFID) sensor data; (v) Interest and behavioral data such as history of websites visited and number of clicks on advertisements, which may include searches on sensitive topics such as health issues or religious views, games and apps used, telecommunications data from car insurance companies, social media posts, professional websites, email exchanges; (vi) Financial transaction data such as history from utility providers, service contract details, income and credit rating information, loyalty card purchase history, prices paid, income and credit rating information; (vii) Social media data such as profile information and posts, connections between family members and friends, photos, videos; (viii) Public records such as birth records, death records, marriage records, land registration records.

Personal data can also be distinguished into first-party and third-party data. Among them: (i) First-party data is collected by businesses directly from their audiences and customers, that is, from individuals who have direct interactions with them, such as in a commercial transaction; (ii) Third-party data can be obtained from the first party or other third parties through purchase or exchange. Third-party data can also be collected from public records or analyzing social media. Finally, they can be collected directly by third parties, who collect data directly when users visit the first-party website. Finally, the GDPR divides personal data into ordinary and sensitive personal data. Much of the data collected for advertising purposes can reveal sensitive personal information about consumers. Therefore, personal data protection can be understood as legal protection for data subjects about data processing by another individual or organization.

1.1. Overview of online behavioral advertising

Online behavioral advertising emerged due to the convergence of the trend of information being freely available and online services being freely accessible to Internet users. [1]. Unlike traditional advertising, online behavioral advertising has a decisive advantage in targeting advertising based on Internet users' personal information. Initially, targeting based on Internet users' personal information occurred by displaying ads relevant to the Web page being browsed or the Web search that had just been performed. However, new technologies have quickly become able to collect much more personal information as the Internet has expanded into a popular medium for providing any service by considering demographic profiles such as gender, age, and interests. Records of past Internet users' behavior can be used to establish correlations between personal data about purchases made, websites visited, social media likes, etc. The increasing effectiveness of online behavioral advertising has provided an enormous incentive for monitoring and collecting massive amounts of personal data. All online activity, every click or message, can be recorded, and valuable correlations can be connected to the most effective online behavioral advertising. In the Internet of Things context, physical objects such as home appliances, cars, televisions, smart refrigerators, etc., are equipped with sensing and computing capabilities that allow the collection of vast amounts of data.[2] Online behavioral advertising targets are determined based on personal information provided or personal information collected through the online behavior of Internet users. According to the European Commission, online behavioral advertising includes:[3] (i) Advertising based on the content of the website visited or the keywords entered into the search engine; (ii) Advertising based on information provided by the individual when registering on a website, such as gender, age, or location; (iii) Advertising based on observing the behavior of individuals over time through the behavior of accessing the website repeatedly, interacting, keywords, producing online content... to develop a specific profile to provide individuals with advertisements

[1] Castells, M. (2001). *The Internet Galaxy*, Oxford University Press, p. 27

[2] Helberger, N. (2016). *Digital Revolution: Challenges for Contract Law in Practice*, Hart Publishing, p 135–161.

[3]European Commission (2018). Consumer market study on online market segmentation through personalized pricing/offers in the European Union, https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalized -pricing offers-European-union_en

tailored to their interests. Online behavioral advertising can be understood as using personal data to select and display digital content to introduce goods, services, or traders of goods and services to Internet users. The online behavioral advertising market aims to match advertising with Internet users by applying personal data processing procedures based on various technologies. Data processing includes any operation performed on personal data such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, blocking, deletion, or destruction of such data.[4] Online behavioral advertising provides Internet users with more personalized, relevant, and engaging advertising content to improve the online experience of consumers. While in the past, Internet users only passively read from a few local media, today, people can search for news according to their interests from many different sources in a much more active way.[5] The Internet's filtering mechanisms determine what users see, whether user-selected or algorithmically chosen. Online behavioral advertising has been hailed as a significant contribution to the technological revolution.[6] but also considered untrustworthy.[7] Trade associations representing the advertising industry often claim that the entire Internet ecosystem is supported by online behavioral advertising.[8] After all, without the constant flow of money from online behavioral advertising, all the free services, news, videos, and apps would disappear.[9] Online behavioral advertising publishers argue that tracking, profiling, and targeting are simply about better understanding customers, directly providing them with tailored services, and placing appropriate ads in front of Internet users. Online behavioral advertising companies often use data collection and processing methods that violate Internet users' rights when extracting and analyzing personal data for online behavioral advertising tracking and profiling. These risks can include discrimination, inequality, stereotyping, stigma, and inaccuracy in decision-making. According to Hildebrant [10], the increasing relevance of tracking, data analysis, and personal profiling technologies in the overall development of digital technology puts society at risk of becoming dependent and unable to control the process and impact of technology. According to Shoshanna Zubbof, the

[4] The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and on the free movement of such data*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[5] Emily Bell, C.W. Anderson & Clay Shirky (2012). " Post-Industrial Journalism: Adapting to the Present," *Columbia Journal Review*, https://www.cjr.org/behind_the_news/post_industrial_journalism_ada.php

[6] Steven Levy (2011). *In the Plex: How Google Thinks, Works, and Shapes Our Lives,* Publisher Simon & Schuster, p. 3.

[7] Scott Cleland (2011). *Search & Destroy: Why You Cannot Trust Google Inc,* Publisher Telescope Books, p. 20.

[8] IAB Europe (2010), *Consumers Driving the Digital Uptake: The Economic Value of Online AdvertisingBased Services for Consumers* (2010), https://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf

[9]Internet Advertising Bureau UK (2014), *The Data Deal: How Data-Driven Digital Advertising Benefits UK Citizens*, https://www.iabuk.com/policy/data-deal-how-data-driven-digital-advertising-benefits-uk -citizens

[10]Mireille Hildebrandt (2009). *Profiling and the rule of law*, Publishing House. Springer, p. 36.

risk increases by developing unexpected and confusing exploitation and control mechanisms that make people distance themselves from their behavior.[11] The legitimate rights and interests of individuals will not be guaranteed because online behavioral advertising companies regularly track and profile Internet users.[12] Experts say that online behavioral advertising is the tip of the iceberg.[13] Because it is the starting point of massive data collection, which, at a high level, can lead to the control of human behavior, the entire online behavioral advertising market is aimed at combining advertising with users. To achieve this goal, various data-intensive and technology-based processes will be deployed and distributed across market participants. The value creation process is data-centric, from monitoring users' online activities to serving advertisements on the advertiser's website, and relies on powerful analytics and intelligent computing technologies. Information can be collected through a variety of online tracking and data-matching technologies. Tracking can involve extensive monitoring of people's behavior, potentially leading to surveillance by subjects that increase the risk of loss of Privacy, discrimination, and identity theft of Internet users45. Web Cookies, Cookie Walls, Hidden Cookies, Web Beacons, and Device Fingerprinting are the most widely used tracking technologies.

2. THE IMPACT OF ONLINE BEHAVIORAL ADVERTISING ON HUMAN RIGHTS

2.1. Online behavioral advertising invades Privacy

In 1890, Warren and Brandeis referred to the right to Privacy about the invasion of private and family life by the press.[14] The invasion involved journalists increasingly interested in gossiping about a person's private relationships and ended up with the mental anguish of those whose information was unwittingly made public. According to Warren and Brandeis, Privacy has two characteristics: the flow of personal information and damage to a person's personality. Privacy must be protected by law because of a person's natural desire to avoid public scrutiny. In 1960, Prosser conducted an extensive review of US court decisions that involved the right to Privacy and summarized four forms of invasion of Privacy: intrusion, public disclosure of personal information, false display of personal information to the public, and improper use of personal information.[15] Except for the first, the other three invasions are all related to Warren and Brandeis's concept of Privacy as the flow of personal information. The first is an invasion of Privacy or private matters that do not require disclosure. According to Warren and Brandeis, wiretapping is not covered by privacy laws. Conversely, according to Prosser, an unlawful search of a person's shopping bag in a store would also invade Privacy.

The Internet has provided an unprecedented space for new forms of advertising to flourish and for ordinary people to collect and share information at a meager cost. While newspapers in the late 19th century were the only ones who could effectively discover and disseminate personal stories, the ease with which personal data can be collected and processed has empowered almost anyone to do so.[16] So, how can privacy threats to big

[11] Zuboff Shoshana (2015). "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology* , 30(1), p. 75–89.

[12] Zuboff Shoshana (2015), “Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology* , 30(1), p. 75–89.

[13] Zuiderveen Borgesius Frederik (2016), "Singling out people without knowing their names – Behavioral targeting, pseudonymous data, and the new Data Protection Regulation," *Computer Law & Security Review*, 32(2), p. 256-271.

[14] Samuel D. Warren and Louis D. Brandeis (1890). "The Right to Privacy," *Harvard Law Review*, 04, p. 193.

[15] William L. Prosser (1960). "Privacy", *California Law Review*, 08, p. 383.

[16] Kim McNamara (2011). "The Paparazzi Industry and New Media: The Evolving

data, often associated with processing personal data, be compromised? Tene and Polonetsky develop the concept of a piecemeal process through which profiles relating to individuals can become more visible as personal data accumulates. Ohm argues that if separate pieces of information from an anonymized database are entirely linked, they can be unlocked if just one of those pieces is linked to a person's real identity, ending up with a vast database.[17] For example 2006, AOL published a list of 20 million de-identified search queries with only a random ID assigned to each searcher. Shortly after publication, The New York Times identified a woman as "*User 4417749* " using only a few keywords, such as "*numb fingers*" and "*60 single men.*"[18] Armed with a massive database of detailed personal information and data mining technologies, any organization or individual can quickly learn about their jobs, leisure activities, favorite supermarkets, or other sensitive information such as medical conditions, sexual orientation, and religious views.[19] Thus, tracking a person's online activities is like paparazzi taking photos of a celebrity's home.

The European Convention on Human Rights (ECHR) does not use the term right to Privacy. However, Article 8 of the Convention provides the right to respect private life, family, home, and correspondence. Similarly, Article 7 of the Charter of Fundamental Rights of the European Union provides the right to respect private and family life, home, and communications. At the national level, the constitutions of many European countries have incorporated the protection of Privacy or private family life as a fundamental right.[20] Article 7 of the Charter provides for the right to Privacy, while Article 8 of the Charter provides for the right to data protection.[21] Therefore, when considering privacy issues from a European perspective, Privacy and data protection are considered separate but related. Similarly, Article 1(1) of the Data Protection Directive (DPD)

Production and Consumption of Celebrity News and Gossip Websites", *International Journal of Cultural Studies*, 14(5), 515.

[17] Paul Ohm (2010). "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, 57, 1746-1748.

[18] Michael Barbaro and Tom Zeller Jr. (2006). "A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times,* *https://www.nytimes.com/2006/08/09/technology/09aol.html*.

[19]Carter Jernigan and Behram FT Mistree (2009). *Gaydar: Facebook Friendships Exposing Sexual Orientation*, https://firstmonday.org/ojs/index.php/fm/article/view/2611

[20]These include the Belgian Constitution [2014], article 22; the Bulgarian Constitution [2007], article 32;
Constitution of Croatia [2010], article 35; Constitution of Estonia [2011], article 26; Constitution of Finland [2011], page 10; Constitution of Greece [2008], article 9; Constitution of Hungary [2011], art VI; Constitution of Latvia [2014], article 96; Constitution of Lithuania [2006], article 22; Constitution of the Netherlands [2008], article 10; Constitution of Poland [2009], article 47; Constitution of Portugal [2005], article 26(1); Constitution of Romania [2003], article 26; Constitution of Slovakia [2014], article 19; Constitution of Spain [2011], page 18. English versions of these Constitutions are available at https://www.constituteproject.org/?lang=en

[21]Article 7 on Respect for Private Life and Family provides: " *Everyone has the right to respect for his or her private and family life, home and communications*. " Article 8 on Personal Data Protection provides: " *Everyone has the right to the protection of personal data concerning him or her*. "

provides for the right to Privacy concerning the processing of personal data[22], while Article 1(2) of the General Data Protection Regulation (GPDR) uses the term right to personal data protection.[23]

A study of the history of the emergence of personal data protection as a fundamental right argues that the association or separation of data protection from the concept of Privacy is artificial.[24] The 1970s saw a wave of European national legislation regulating the processing of personal data without explicitly mentioning the goal of protecting Privacy. In the process of drafting international documents and instruments related to data processing and the free movement of data [25], the term " *data protection*" was adopted in its whole meaning – that is, the principles of automated processing of personal data, thereby making personal data protection a separate area of law.[26] However, as Westin defines Privacy as the ability to determine the transmission of information about oneself, the processing of personally identifiable information by computer would be addressed by extending the concept of "*privacy*" to include what is known as "*information security*".[27] The convergence of "*personal data protection*" and "*privacy*" in international documents has profoundly impacted subsequent legislation at the EU and national levels. For example, the DPD and the ePrivacy Directive were created in a way that highlights "*privacy*".[28] The ambiguity and frequent misuse of the concept of "*privacy*" in various contexts, such as "*respect for private life*" in the ECHR, "*the right to be left alone*" in the mainstream American understanding, and "*control over personal data*" in the updated definition, have primarily led to severe confusion about the relationship between "*data protection*" and "*privacy*." Today, the Charter of Fundamental Rights of the European Union (CFR) and the GDPR deliberately signify a departure from the concept of Privacy, with the term "*protection of personal data*" being preferred. Despite the similarities, in the case of data processing through new technologies, some features still differ from what was experienced a century ago, such as the degree of human intervention and the expected scope of the privacy domain.

In the case of online behavioral advertising, Internet user data is almost always collected and analyzed in a fully automated manner. However, the traditional idea of Privacy underpins the rationale for providing legal protection for personal information based on the assumption that people care about how others perceive them. Here, "*others*" can be just one person – in the case of wiretapping or many unidentifiable people – in

---

[22] The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and on the free movement of such data*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.

[23] The European Parliament (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General et al.) (Text with EEA relevance)*, https://eur-lex.europa.eu/eli/reg/2016/679/oj

[24] Gloria González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, p. 254–257.

[25] OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy -and-transborder-flows-of-personal-data_9789264196391-en

[26] Gloria González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, p. 254–257.

[27] Alan F. Westin (2015). *Privacy and Freedom,* Ig Publishing, p. 102-105

[28] Body present in section gender Introduction and Article 1 of two Only markets, also like pepper subject belong to Only market About Privacy private and transmit information electricity death

the case of media disclosure, and the subject must be a human rather than a machine. It can be argued that computers do not violate privacy; only humans do. Privacy is only threatened when another person observes a person, so processing by wholly automated means should not be considered a threat to Privacy. From a technical perspective, online behavioral advertisers can do what The New York Times does with their massive database, but they have little interest in tracking individual customer data. Some forms of automated processing of personal data are more sensitive and may require human oversight.

On the other hand, in online behavioral advertising, the scope of private space in the traditional sense of Privacy needs to be clarified. A person's desire to avoid public contact should be respected. Therefore, what a person does, says, writes, or expresses in a relatively private place such as a home, dressing room, meeting room, or sealed letter in an envelope is not subject to surveillance or publicity. In the Internet environment, when a user accesses a website by connecting the device to a remote server via the Internet, to what extent can the user's "*private space*" be extended? Some may regard online tracking as an observation of an individual's private life because the way a person uses the device, in most cases, is not allowed to be shared with others.

On the other hand, in addition to the websites users want to visit, other third parties are involved in the tracking, profiling, and targeting process. Most of these activities are not carried out directly between services but through the Internet user's browser. Technically, the communications are "*requested*" by the browser in response to instructions programmed by the Web page. Should this be considered part of a person's "*private and family life*" as defined in the ECHR or the Charter, or within the private sphere of a person's "*leaving alone*" as defined by Warren and Brandeis? From different perspectives, there can be opposing interpretations that lead to opposite perceptions of the extent to which the rights of Internet users are violated. Even if the interaction between a user and a Web page were protected as private and confidential, the interference of third-party trackers would no longer be considered private. Theoretically, the most common form of third-party tracking can only occur with permission from the web page and the browser. However, a counter-argument is that the average user, in most cases, needs to be made aware of third-party tracking, does not have the skills to turn off tracking, or is concerned about the limited functionality. Hence, their expectation remains that communications should be protected as private conversations.

There is no comparable case where the divide between private and public in the real world can be fully understood in the online environment. That is why the traditional concept of Privacy is difficult to apply. American judges and scholars are still debating whether the dissemination of location data on smartphones should be considered "*public, voluntary activities*" and, therefore, not protected by the US Fourth Amendment.[29] This also explains why the idea that one can be "*private in public*" is largely rejected in the US.[30] It is readily accepted in Europe.[31] In the Internet environment, the line between private and non-private is no longer clear, especially in the case of online behavioral advertising.[32] The user's electronic device is an arm extension that can reach others. However, electronic devices are also an extension of the arm that allows others to reach Internet users.

The blurred boundaries between the parties are a product of the infrastructure and standardization of the Internet. Cookie standards and the HTTP protocol have primarily determined the direction of the flow of

[29]Monu Bedi (2016). " The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-up ", *Northwestern University Law Review*, 110(2), p. 507.

[30] Ronald J. Krotoszynski, Jr. (2016). *Privacy Revisited: A Global Perspective on the Right to Be Left Alone,* Publishing House Oxford University Press, page 5.

[31]NA Moreham (2006). "Privacy in Public Places," *Cambridge Law Journal*, p. 606.

[32]Daniel J. Solove (2010). *Understanding Privacy,* Harvard University Press, 65(3) page 24

data and the availability of that data on demand.[33] The configuration of the Internet is thus two-way but asymmetric. The use of Cookies has dramatically enhanced the user experience and created new forms of interaction. However, the Internet has also forced the device to follow the Web page's instructions for the benefit of the Internet user himself. However, the ability of the Internet user to exercise choice is mainly dependent on technical, economic, and social factors. On the technical side, reverse tracking techniques are available but are only sometimes practical. On the one hand, it is possible to bypass disabled or deleted Cookies using new tracking devices, including Flash Cookies, mobile phone unique IDs, or other forms of device fingerprinting that allow "*Cookie recovery*."[34] On the other hand, despite the availability of intelligent software to block online tracking, companies are consistently deploying solutions to combat online behavioral ad-blocking.[35] Economically, Internet users may face an unpleasant, uninformed browsing experience or be denied access to services altogether if they turn off cookies or use anti-tracking software.[36] Socially, certain services may form such an essential part of a group of people's digital society that opting out of services to prevent behavioral tracking is not an option.[37] So, technical, economic, and social factors tip the balance of online behavioral trackers. These factors have a decisive impact on what people expect to be private or public, but the problem is that these factors tend to be pervasive online. The boundaries of walls and envelopes are more easily defined than those related to online tracking technology. The essential concept of Privacy draws a line separating a person's private life from his or her public life. Information within the private sphere needs to be protected from unauthorized observation and circulation. Individuals effectively manage their public presence by controlling the information that can reach the public sphere. The classic definition of Privacy as "*the right to be left alone*" does not imply that individuals do not care about their public life. Instead, individuals are more likely to want to be alone occasionally because they know they will eventually need to return to public life and do not want privacy issues to interfere once they enter public life. Thus, Privacy may maintain a positive or non-negative image of the public aspect of life.

In the Internet age, apart from a good image in real life, people who want to connect positively with others also need to maintain a polite personal presence on the Internet. Nowadays, it is widespread for corporations to use mass media, corporate media, and social media to build and maintain their corporate reputation. Similarly, Facebook and X posts have become popular as a means to enhance their professional presence and influence in the public. Most Internet users build online profiles to impress their friends or society. It is a strategy to create an attractive impression on others, such as family, friends, colleagues, leaders, fans, customers, or anyone interested in the person. Maintaining a good image is the primary purpose of managing one's offline and online presence. The case of online behavioral advertising, however, involves reputation in a less immediate but more subtle way. One of the difficulties in applying traditional privacy theory to the case of online behavioral advertising is that human observation is significantly reduced. If being observed by an

[33]Paul M. Schwartz (1999). " Privacy and Democracy in Cyberspace," *Vanderbilt Law Review*, 52, p. 1607.

[34]Omer Tene & Jules Polonetsky (2012). "To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising," *Minnesota Journal of Law, Science & Technology*, 13, p. 281.

[35]Rishab Nithyanand and add (2016), *Adblocking and Counter-Blocking: A Slice of the Arms Race*, https://www.usenix.org/system/files/conference/foci16/foci16-paper-nithyanand.pdf

[36]Ashkan Soltani and Add (2009). Flash *Cookies and Privacy*, https://typeset.io/pdf/flash-cookies-and-privacy-3nekb4ffz4.pdf

[37]Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson, and Council on Communications and Media (2011), "Clinical Report—The Impact of Social Media on Children, Adolescents, and Families," *Pediatrics*, 127(4), p. 800.

insect on the wall is not a privacy issue, then being observed by a computer system is not. In The Black Box Society, Pasquale uses the concept of "*digital reputation*" to demonstrate the threats we face today in the "*data age*." He looks at the latest trends and uses scoring technology in the financial and medical fields. The use of credit scores and medical records are, of course, notorious examples of the potential tarnishing effects on a person's reputation.

With the proliferation of online behavioral advertising, digital reputations are becoming increasingly challenging to manage, and user profiles can be merged with private profiles, public profiles, and even the profiles of others. The wall between private and public has disappeared mainly in the online world. The Internet structure makes it easier for advertisers to build user profiles but does not allow users to manage that presence. If creating a technological item unfairly unbalances the current distribution of benefits, then a reformulation of the relevant legal policy is necessary. An electronic device is the property of its owner, but it serves the owner and online behavioral advertisers. Tracking, profiling, and targeting are all done in a decentralized, multi-level manner. Advertisers, publishers, and advertising service providers can store a user's profile. To such an extent, big data has made the reputation of the individual data subject completely unmanageable. Because if credit scoring were based solely on credit history, individuals could quickly figure out how to avoid negative factors or what went wrong when something went wrong. However, a person cannot check the scoring system when it is based on a complex set of data connected to private activity, hidden records, external sources, and other customers.

2.2. Online behavioral advertising violates the right to information autonomy

In 1983, the German Federal Constitutional Court ruled that individuals' freedom to decide whether to engage in certain activities may be limited if they cannot determine when and who knows what about them.[38] Similarly, the Portuguese Constitution prohibits the processing of personal data not only in private life but also in religious beliefs.[39] Before the German court's ruling, there was academic discussion of a new model for Privacy. Westin argued that Privacy is the claim of individuals, groups, or organizations to determine when, how, and to what extent information about them is communicated to others.[40] Fried argued that Privacy is not simply the absence of personal information in the minds of others but rather an individual's control over information about himself.[41] The ability to control one's information is essential because if the information is beyond the social context in which its meaning is expressed correctly, it can be inconvenient[42] and prevent an individual from saying something that is not morally wrong but is unpopular or unconventional.[43] Thus, the reason of the law for granting control over personal data is not much different from granting property rights when voluntary exchange can help achieve an optimal equilibrium.[44] To this extent, economic theories of informational autonomy have some common ground. If individuals do not have

---

[38] The Fed er al Con sti tu tion al Court (1965), *BVerfGE 65, 1 [1965] s II. 1. A* , https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/12/rs19991215_1bvr065396en.html

[39]Portuguese Assembly (1976), The Constitution of Portugal, https://www.constituteproject.org/constitution/Portugal_2005

[40] Alan F. Westin (2015). *Privacy and Freedom,* Ig Publishing, p. 374.

[41] Charles Fried (1968). " Privacy, *"The Yale Law Journal*, p. 475, 482.

[42] According to Nissenbaum's theory, 'contextual integrity' is violated. See Helen Nissenbaum (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Publishing House Stanford University Press, p. 140.

[43] Charles Fried (1968). " Privacy, *"The Yale Law Journal*, p. 483–484.

[44] Richard A. Posner (1978). "The Right of Privacy", *Georgia Law Review*, 12(3), p. 397.

control over their data, they are more likely to try to keep the information to themselves. While Fried calls this an unjust restriction on free speech, Posner argues that it is a suboptimal condition that hinders the provision and transmission of valuable information.

The ability to control information is a prerequisite for forming a unique "*self*" in a relatively homogeneous social context. Lynskey argues that an individual's public information can have many aspects, the combination of which can hinder their self-development.[45] Similarly, Rouvroy and Poullet have pointed out the importance of informational autonomy as an absolute element in a person's personality and the construction of personal identity.[46] Cohen sees Privacy as a comfortable space for individuals' personalities to form.[47] Posner argues that forced disclosure of personal information is sometimes desirable if the nature of the information will lead to external effects or if the transaction costs of voluntary information collection are too high.[48] Solove also advocates a similar approach, arguing that privacy issues should be decided based on a balance of interests from both sides.[49] At the same time, forming personal characteristics is not just a product of individual subjectivity. Social patterns and constraints also play an essential role in maintaining a stable society. Therefore, Cohen observes that subjectivity will emerge "*gradually, in significantly constrained ways but not rigidly determined by social shaping*".[50] Internet users currently have little control over data collected from themselves. In the era before online behavioral advertising, marketing research was conducted primarily through surveys. Consumers could decide whether to participate in any survey and what answers to give to each question. In contrast, online behavioral data is collected automatically with only the best protections of "*opt-out*" or "*implied consent*." There is no easy way to tailor the data to an individual's wishes before sending it.

Furthermore, once data is collected by advertisers, publishers, or ad vendors, it is entirely out of the user's control. The whole idea of big data is to maximize the collection and analysis of data, regardless of how it is collected. This lack of control is present throughout the entire online behavioral advertising operation. During the tracking phase, only IT professionals know how to manage the data flow to determine what data about users is collected. For the profiling stage, the complexity of big data algorithms, combined with the need for more transparency, will make it extremely difficult for users to find out what profiles have been built and what automated assessments, predictions, or decisions have been made based on those profiles. [51]. Individuals may be subjected to algorithmic systems where data is secretly collected and used to inform some

---

[45]Orla Lynskey (2014). "Deconstructing Data Protection: The "Added-value" of a Right to Data
Protection in the EU Legal Order", *International and Comparative Law Quarterly,* 63 (3), p. 569-597.

[46] Antoinette Rouvroy and Yves Poullet (2009) , *Reinventing Data Protection?* , Springer Publishing House, p. 51.

[47] Julie E. Cohen (2013). "What Privacy Is For", *Harvard Law Review*, 126(7), p. 1927-1932.

[48] Richard A. Posner (1978). "The Right of Privacy", *Georgia Law Review*, 12(3), p. 397–401.

[49] Daniel J. Solove (2009). *Understanding Privacy,* Publishing House. Harvard University Press, p. 50.

[50]Julie E. Cohen (2013). "What Privacy Is For," *Harvard Law Review*, 126(7), p. 1910.

[51] See more: Download Your Data, access access in https://support.google.com/accounts/answer/3024190, and How Can I Download My Information from Facebook? Tru access at https://www.facebook.com/help/212802592074644

form of decision-making without their content being confusing to people.[52] Posner has demonstrated from an economic perspective that making one's data public can be seen as a way to manipulate information about that person.[53] Manipulation is only sometimes something entirely negative. Posner believes that others can demand an individual's private information as a demand for information about an asset to inform their decision-making process.[54]

2.3. Online behavioral advertising violates the autonomy.

Personal autonomy is understood in the sense that an individual is autonomous in society, meaning that he or she possesses the necessary conditions to make essential decisions in life.[55] Minors are often not considered to be fully autonomous[56] because they are assumed to lack the intellectual maturity to make informed decisions. Enslaved people are incapable of autonomy because they do not enjoy the necessary freedom to act as they wish.[57] People with no savings can hardly claim autonomy because they do not have the minimum tools to exercise even the most limited choices.[58] Among the critical factors that make a person autonomous, the ability to control personal information is becoming more critical than ever in contemporary society. Recalling what the German Constitutional Court stated in the case of confirming the right to informational self-determination, this is even clearer.[59] If, at the time, collecting demographic information about citizens in a national census could be seen as a potential interference with individual autonomy, today's widespread tracking activities on the Internet are even more worrying.

In the past, people needed Privacy because otherwise, they would be subjected to constant observation and judgment, which greatly limited their choices about what they could do comfortably. With adequate control over personal data, people would know that their decision-making might have been compromised. Individuals would be subject to manipulation by data holders if personal data were used without the supervision of the data subject. Companies in the online behavioral advertising industry have the technological power to analyze user behavior precisely to better personalize content to target users. In a world without regulations on the use of personal data, individuals would be vulnerable to influence. They would not be able to make their own decisions genuinely autonomously.

In contemporary life, informational self-determination is integral to autonomy, especially regarding data use activities. In other words, in a data society, individuals cannot have autonomy without effective informational

---

[52] John Danaher (2016). " The Threat of Algocracy: Reality, Resistance and Accommodation ", *Philosophy & Technology*, 29, p. 245.

[53] Richard A. Posner (1978). "The Right of Privacy", *Georgia Law Review*, 12(3), p. 39 3.

[54] Richard A. Posner (1978). "The Right of Privacy", *Georgia Law Review*, 12(3), p. 39 6.

[55] Joseph Raz (1988). *The Morality of Freedom,* Publishing House. Oxford University Press, p. 369.

[56] Gerald Dworkin (1988), *The Theory and Practice of Autonomy,* Publishing House. Cambridge University Press, p. 9.

[57] Gerald Dworkin (1988). *The Theory and Practice of Autonomy,* Publishing House Cambridge University Press, p. 129.

[58] NE Simmonds (1981). " Property, Autonomy and Welfare ", *ARSP*, 67(1), p. 61, 66.

[59] The Fed er al Con sti tu tion al Court (1965), *BVerfGE 65, 1 [1965] s II. 1. A* , https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/12/rs19991215_1bvr065396en.html

self-determination.[60] However, it is important to emphasize that there is an essential distinction between self-determination and informational autonomy.[61] That leads to more complex issues about the nature of autonomy. Informational self-determination is primarily concerned with a person's control over personal information.[62] On the other hand, autonomy is more about choosing one's life principles. DeterminingDetermining what happens to one's data is one of the approaches to autonomy.

Online behavioral advertising can threaten a person's autonomy when data subjects cannot consciously identify themselves as being tracked online. The principle of equality can also be undermined by unfair treatment based on the use of personal data. Unfairness can arise from inaccurate information or overly general classifications on the one hand, from accurate but unverifiable information, and more apparent distinctions on the other.[63] All of these potential adverse effects can pose severe risks to data subjects. As personal data becomes more widely used, a helpful approach to maintaining autonomy is to address the issue of liberty and equality in the context of big data. It is easy to see why autonomy lies at the heart of liberty and equality. As Rawls paraphrases Kant's concept of autonomy, "*A man is acting autonomously when the principles of action he chooses are the fullest expression of his nature as a rational, accessible, and equal being*". [64]The values of freedom and equality are inherently linked to autonomy.[65] A man who acts under external influence cannot be said to act autonomously. Benn presents a view of an autonomous man as one whose consistent life is rooted in a set of beliefs, values, and principles by which his actions are regulated.[66] For him, choice and rational criticism are necessary conditions for autonomy[67], stating that "*being a chooser is not enough to be autonomous*".[68]

---

[60] Eoin Carolan and Alessandro Spina (2015). *Nudge and the Law: A European Perspective,* Publishing House Hart Publishing, pp. 165-166.

[61]Woodrow Hartzog (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies,* Publishing House. Harvard University Press, p. 118–119.

[62] Claudia Quelle (2016). Privacy and Identity Management: Facing up to Next Steps, Publishing House. Springer, p . 144; Sophie C. Boerman, Sanne Kruikemeier and Frederik J. Zuiderveen Borgesius (2017) , " Online Behavioral Advertising: A Literature Review and Research Agenda , " *Journal of Advertising* , 46(3), p . 363 - 374.

[63] Jiahong Chen (2018). "The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle," *European Data Protection Law Review*, 4, p. 36.

[64] John Rawls (2009). *A Theory of Justice*, Publishing House. Harvard University Press, p. 222.

[65] Gerald Dworkin (1988). *The Theory and Practice of Autonomy,* Publishing House. Cambridge University Press, p. 12–20.

[66] SI Benn (1976). "Freedom, Autonomy and the Concept of a Person," *Proceedings of the Aristotelian Society*, 76(1), p. 124.

[67] SI Benn (1976). "Freedom, Autonomy and the Concept of a Person", *Proceedings of the Aristotelian Society*, 76(1), p. 12 7.

[68] SI Benn (1976). "Freedom, Autonomy and the Concept of a Person", *Proceedings of the Aristotelian Society*, 76(1), p. 12 3

With another approach, Raz presents the essence of personal autonomy as "*the vision of those who control, to some extent, the destiny of the individual himself, shaping the individual himself through successive decisions throughout his life*."[69] To satisfy the element of autonomy, three conditions must be met: minimal mental capacity, full range of choices, and independence from coercion.[70] For Raz, "*the environment in which autonomous life can develop* "is essential for achieving autonomy.[71] Accordingly, a desirable model of freedom must be one that " *protects those pursuing different lifestyles from intolerance and calls for the provision of conditions of autonomy without which autonomous living is impossible*".[72] Between these two approaches lies Dworkin's theory of autonomy, which focuses heavily on the individual's ability to reflect on life decisions. He sees autonomy as an intermediary between a person's particular preferences and the general, principled values that the person possesses. For him, autonomy is conceived as a second-order human capacity to critically reflect on preferences and desires and accept or attempt to change these by higher-order preferences. By exercising such a capacity, humans define their nature, give meaning and coherence to their lives, and take responsibility for who they are.[73] Dworkin points out that: "*a state may be required to recognize the autonomy of its citizens. That is, it may only restrict the freedom of individuals if it can justify such restrictions by arguments that the individual himself can consider accurate*".[74] Raz's theory may be intrinsically relevant to data protection because it views autonomy as a matter of lifestyle rather than specific decisions. The emphasis on the role and limitations of law in promoting autonomy fits well with the ongoing debate about the model of data protection law. Much of Raz's work on legal theories concerns the seemingly conflicting normative requirements of human reason and authority. In short, his question is if the nature of law requires that organizations and individuals in society obey it without questioning its rationale, how can this be compatible with human autonomy?[75] In everyday life, it is not uncommon for us to give up our final decision-making power or limit our future choices by, for example, committing to a contract, setting a speed limit, etc.[76] The point is that there are many other ways to achieve the fundamental value of being able to act on our judgment by reason.[77] For Raz, obedience to authority "*is not a denial of people's ability to act rationally, but simply a means if the authority allows*

---

[69] Joseph Raz (1988). *The Morality of Freedom,* Publishing House. Oxford University Press, p. 369.

[70] Joseph Raz (1988). *The Morality of Freedom,* Publishing House. Oxford University Press, p. 369–378.

[71]Joseph Raz (1988). *The Morality of Freedom,* Publishing House. Oxford University Press, p. 391.

[72] Joseph Raz (1988). *The Morality of Freedom*, Publishing House. Oxford University Press, p. 425.

[73] Gerald Dworkin (1988). *The Theory and Practice of Autonomy,* Publishing House. Cambridge University Press, p. 20.

[74] Gerald Dworkin (1988). *The Theory and Practice of Autonomy,* Publishing House. Cambridge University Press, p. 40.

[75] Joseph Raz (2009). *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House. Oxford University Press, p. 135.

[76] Joseph Raz (2009). *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House. Oxford University Press, p. 140.

[77] Joseph Raz (2009). *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House. Oxford University Press, p. 140.

the subject to confirm better reasons".[78] Of course, there are cases where such commitments cannot be considered a tool for rationality. For example, a promise to become enslaved would not be considered an autonomous act based on reason.[79] Similarly, in the context of online behavioral advertising, a person who promises to allow all personal data to be used for any commercial purpose would not be considered to have exercised autonomy.

3. EU LEGAL REGULATION ON CONSENT TO PROCESSING PERSONAL DATA IN ONLINE BEHAVIORAL ADVERTISING

Consent to online behavioral advertising is required on an ongoing basis, and the data controller must justify processing personal data. This is because the processing of personal data affects online purchasing behavior and the user's ability to access information. In today's online behavioral advertising business model, users are pressured to provide personal data to providers and accept being tracked when interacting with online services. The data collected may include personal information entered by users such as name, place of residence, age, gender, etc., as well as online tracking results such as pages visited, buttons clicked, messages posted, etc. Such data can be incorporated into a user profile to infer other user characteristics, such as interests, wealth level, or psychological attitudes. The collected user data and profiles can also be sold on data marketplaces, thus creating a more significant impact on the lives of Internet users.

EU data protection law applies when a company processes "personal data," information relating to an identified or identifiable data subject.[80] The definition of "processing" is comprehensive, and almost anything that can be done with personal data falls within its scope. Online behavioral advertising requires the processing of personal data. Pseudonymized data attached to Cookies are personal because they "*allow data subjects to be identified, even when their real names are* unknown."[81] This is consistent with the case law of the Court of Justice of the European Union.[82] European data protection law applies when a company is established in the European Union. The law also applies if a company is not based in Europe but uses

[78] Joseph Raz (2009). *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House Oxford University Press, p. 140.

[79] Joseph Raz (2009). *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House. Oxford University Press, p. 136.

[80] The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and the free movement of such data*, Article 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

[81]See also " Opinion 2/2010 on online behavioral advertising ", accessed access in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[82] See more: " EFFECTIVE DATA PROTECTION AND FUNDAMENTAL RIGHTS, "access in https://www.fricore.eu/sites/default/files/content/materials/4._fricore_casebook_-_data_protection_isbn_fp_cp_002_dd.pdf

European-based equipment to process data[83] or uses Cookies to track EU citizens.[84] Consent is the sole legal basis for processing personal data collected by Cookies;[85] it is also the sole legal basis for processing data during the tracking period.

Consent is considered the most essential basis under EU personal data protection law.[86] Consent plays a crucial role in the European approach to personal data protection.[87] because it involves individual autonomy in allowing companies to advertise their behavior online in data processing; according to the Task Force, "*consent is related to the concept of informational autonomy. The autonomy of the data subject is both a prerequisite and a consequence of consent, which gives the data subject control over data processing*".[88] Internet users are pressured to provide personal data to providers and to accept tracking when interacting with online services. The GPDR states that affirmative and actual action by the user is necessary to obtain lawful consent.[89] Therefore, pre-ticked boxes or inaction do not constitute consent.[90] Consent applies to each purpose, and the user will be informed about how and for what purposes personal data will be used. The user can also easily withdraw consent at any time. The data controller is burdened to prove that consent has been lawfully obtained. This regulation guarantees Internet users autonomy, giving data subjects more leeway to decide when to share data and for what purposes. The law aims to eliminate the enforceability of implied consent through default settings, instead requiring users to express explicit consent. However, in the online context, consent is often "*as much about an intuitive response to specific cues as it is about thoughtful and deliberate thinking*." According to Koops, consent is essentially a theory that denies the reality of 21st-century data processing.[91] Internet users must often read terms and conditions or pop-up banners in their browsers. The ease of dismissing banners through the "*I agree*" click option often results in individuals explicitly agreeing to agreements to execute

[83] Moerel L (2012), *Binding Corporate Rules: Corporate Self-regulation of Global Data Transfers, Dai University of Tilburg, p. 72.*

[84]See more: " Opinion 1/2008 on data protection issues related to search engines", retrieval access in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

[85] Article 5 (e) of the ePrivacy Directive.

[86]See also: " Opinion 15/2011 on the definition of consent", accessed access in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

[87] Eoin Carolan (2016), "The continuing problems with online consent under the EU's emerging data protection principles," *Computer Law & Security Review*, 32(3), p. 462-473

[88]The European Commission (2011), *Opinion 15/2011 on the definition of consent*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

[89]The European Parliament (2016), *General Data Protection Regulation* (GDPR), Para 32, https://gdpr-info.eu/

[90] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Para 32, https://gdpr-info.eu/

[91] BJ Koops (2014), "The trouble with European data protection law", *International Data Privacy Law*, p. 251.

clickwrap agreements, end user license agreements (EULAs), and downloading applications granting any permissions requested.[92]

Under Clause 11, Article 4, According to the GDPR, consent is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject*."[93] In practice, Internet users need to express their consent to access online services. This makes it mandatory for data subjects to consent and prevents them from exercising their right to withdraw consent or object to data processing. The GDPR also establishes stricter requirements for legal consent regarding children's data, sensitive data, and data used in automated decision-making. The GDPR requires that consent be a freely given, specific, informed, and unambiguous indication, by a statement or by an explicit affirmative action, by the data subject. Consent must be specific, comprehensive, based on clear and specific requirements, and be demonstrable by the controller. Specifically, consent must be freely given, consent must be specific, consent must be informed, and consent must be unambiguous.

3.1. Consent must be freely given

First of all, consent must be "*freely given*". Previously, the DPD did not provide criteria for what constitutes or does not constitute "*freely given*" consent. However, the GDPR has clarified that "*consent is not considered to be freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent without detriment*."[94] The Taskforce considers that "*if the data subject does not have a genuine choice, feels obliged to give consent or would suffer negative consequences if they do not give consent, then the consent is invalid*." [95]. The requirements of consent must include (i) the availability of appropriate options and (ii) that withholding consent does not result in detriment. Consent is only considered freely given if the data subject has a genuinely free choice or can refuse or withdraw consent without detriment. Statements of consent prepared in advance by data controllers must be provided in an easily accessible, understandable form using clear, easy-to-understand language. If the data subject's refusal to consent would put them at a disadvantage, then the consent cannot be considered freely given. The Working Group considers that: "*if withdrawing the consent would result in a downgrade of the performance of the service to the detriment of the user, then consent was never lawfully given*."[96]

Article 7.4 of the GDPR provides that: "*When assessing whether consent has been freely given, due regard shall be paid to whether, among other things, the performance of the contract is conditioned on consent to the processing of personal*

---

[92] Omer Tene and Christopher Wolf (2013), "Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent," *Information Security & Privacy News*, p. 19-28

[93] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 4, Section 11, https://gdpr-info.eu/

[94] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 7, https://gdpr-info.eu/

[95] The European Commission (2017), *Guidelines on Automated Individual Decision-making and Profiling for Regulation 2016/679*, p. 10, https://ec.europa.eu/newsroom/article29/items/612053

[96] The European Commission (2017), *Guidelines on Automated Individual Decision-making and Profiling for Regulation 2016/679*, p. 10, https://ec.europa.eu/newsroom/article29/items/612053.

data".[97] In other words, if the processing of personal data is not necessary for providing a service but the provider still requests it as a condition, the consent will be considered invalid because the situation will be subject to "*due regard*. " The draft GDPR proposed that "*the performance of a contract or the provision of a service shall not be conditioned on consent to the processing of data which is not necessary for the performance of the contract or the provision of the service*."[98] This proposal was rejected,[99] but was later reintroduced with softer wording[100] and reworded into the current GDPR.[101] That is, consent to processing personal data for the performance of a contract is only sometimes valid, and the data controller will need to demonstrate a legitimate reason for the data processing request.[102] Therefore, for the consent to be valid, the online behavioral advertising company must demonstrate that if the Internet user expresses a refusal to consent to data processing, the online behavioral advertising company will not deny the service; otherwise, it will lead to the conclusion that this case is not "*freely given consent*."

[97] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 7, Section 4, https://gdpr-info.eu/

[98]The European Parliament (2013), Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and on the free movement of such data (General et al.), p. 72, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011

[99]The European Parliament (2012), **Proposal on the protection of individuals about the processing of personal data and the free movement of such data (General et al.)**, p. 85, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011

[100]The European Parliament (2015), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and on the free movement of such data (General et al.) - Preparation for trilogue, p. 7, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vjzebx068vy6

[101] The European Parliament (2015), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and the free movement of such data (General et al.) - Preparation for trilogue, p . 2, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vjzebx068vy6.

[102] Information Commissioner's Office (2017), *Consultation: GDPR Consent Guidance*, p. 19-21, https://ico.org.uk/media/about-the-ico/consultations/2013610/gdpr-consent-guidance-consultation-form-word-201703.docx

Philipp Hacker (2017), "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things," *International Data Privacy Law*, 7(4), p. 26;

In theory, consent is no different from a contract in that it represents a mutual agreement between the data subject and the data controller on how personal data will be processed. The Task Force suggests that when determining the validity of consent, the requirements set out by other laws should be taken into account.[103] The Task Force states, "*Article 7.4 of the GDPR seeks to ensure that the purpose of processing personal data is not disguised nor is it accompanied by the provision of a service contract for which the personal data are not necessary*."[104] Online behavioral advertising is a separable purpose and is not necessary for the provision of online services [105]. In other words, requiring Internet users to consent to the use of personal data for advertising purposes before being able to access a service would likely violate the provisions of the GDPR [106]. However, Internet users often have to click on links and read in-depth documents to learn about the use of data for online behavioral advertising. For example, Facebook requires users to click on its cookie policy to learn how they may be tracked online. The only alternative is to click the "*manage data settings*" button to navigate through a more complex interface that makes it easier for users to opt out of specific Cookies. Data subjects often need to be allowed to give separate consent for their data to be processed by different parties for online behavioral advertising purposes. In summary, consent is not considered to be freely given in the following cases: (i) There is an imbalance between data subjects and data controllers. Unbalanced situations arise when one party has a dominant market position, as with online behavioral advertising companies.[107] In all these cases, the online behavioral advertising company must demonstrate no risk of "*deception, intimidation, coercion or significant negative consequences if the data subject does not consent*." (ii) the consent given is not sufficiently specific. That is, the personal data subject does not have the opportunity to give separate consent for different personal data processing activities. (iii) Consent to processing personal data is considered a condition of the contract's performance. That is, the performance of the contract, including the provision of services, is entirely dependent on consent, even if such consent is not necessary for the performance of the contract.

[103]The European Commission (2011), *Opinion 15/2011 on the definition of consent*, retrieval access in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

[104] Frederik J Zuiderveen Borgesius (2017), "Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation," *European Data Protection Law Review*, 3(3), p. 360–361.

[105]The European Commission (2014), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, https://ec.europa.eu/justice/article-29/documentation /opinion-recommendation/files/2011/wp187_en.pdf

[106] Frederik J Zuiderveen Borgesius and colleagues (2017), " Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation, *"European Data Protection Law Review*, 3(3), p . 360-361

[107] The European Parliament (2016), *Guidelines on consent under Regulation 2016/679*, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

3.2. Consent must be explicitly given.

The requirement that consent must be given through a specific act was addressed by the ECJ in case C-673/17(57-58)[108]. In it, the Court stated that consent is invalid if information storage or access to information already stored in the Website user's terminal is permitted by a checkbox pre-checked by the service provider, which the user must uncheck to refuse. In this decision, the Court linked affirmative action to specificity, stating that consent must relate specifically to the processing of the data in question and cannot be inferred from the data subject's indication of his or her wishes for other purposes. Consent that is freely given, specific, informed, and unambiguous can only be the user's explicit consent, given with full knowledge of the facts and after providing full information about the use of his or her data. In case C40/17[109], The ECJ dealt with a third-party social add-on (a Facebook-like button) included in a website. The add-on caused the visitor's browser to the website to request content from the owner of the add-on (Facebook) and transmit personal data about the visitor to that owner. The Court affirmed that the website operator should only request consent to transmit the add-on to the owner. This requires the owner of the add-on to specify the legal basis for any further processing. Another relevant case was recently decided by the French Council of State, which heard Google's appeal against a fine imposed by the French National Data Protection Commission (CNIL). The judges upheld the fine, stating that Google violated the requirement that consent must be informed, specific, unambiguous, and based on affirmative action as provided in Article 4 of the GDPR. Users are provided with a pre-ticked box allowing advertising personalization, which is contrary to affirmative action; they cannot easily access the information for processing, which is contrary to the requirement of freedom of expression, and the information is not specific and too vague. Therefore, the processing of user data, especially in the case of online behavioral advertising, lacks a legal basis according to Article 6, GDPR provisions.

3.3. Consent must be given with informed consent

The third criterion for the validity of consent is whether the consent is given "*informed*"? The Task Force explains that: " *for consent to be informed, it is necessary to inform the data subject of certain elements that are important for making a choice and that such information is clear, distinguishable from other matters and provided in an understandable and accessible form*. "The " [110]*informed* "requirement is therefore directly linked to the principles of transparency and purpose limitation as well as the data controller's obligation to provide information.

[108] T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt (2021), *Data Protection: CJEU case law review – 1995-2020*, https://www.dpcuria.eu/case-law-review-1995-2020.pdf

[109] The CJEU Second Chamber (2019), *Fashion ID GmbH & Co. KGVerbraucherzentrale NRW eV* , https://www.5rb.com/case/fashion-id-gmbh-co-kg-v-verbraucherzentrale-nrw-ev/

[110]The European Parliament (2020), *Guidelines 05/2020 on consent under Regulation 2016/679*, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf

There is a close connection and even overlap between the "specific" and "*informed*" requirements[111]. The GDPR stipulates that "*for consent to be informed, the data subject must at least know the identity of the controller and the intended purpose of processing personal data*."[112] On the other hand, the information that the data controller is obliged to provide is broader in scope than what the "*specific*" element requires. According to Article 13 and Article 14 of the GDPR, the data controller must provide details such as: "*information about the data controller; the purposes and legal basis for the processing; the categories of personal data concerned; the identity or categories of data recipients; the period for which the personal data is stored; the right of the data subject to withdraw consent; the existence of automated decision-making and the potential for influence on the data subject*."[113]
All of these elements must be mentioned in the privacy policy for online behavioral advertising. The collection of personal data in online behavioral advertising often occurs not only on the intended website of the user but also on the advertiser's server. Information about the advertiser, the publisher, the advertising service provider, and other relevant parties must be made clear to the data subject, including the scope of the data processed and how the personal data is processed. To express consent, At a minimum, the data subject must know the controller's identity and the purposes for which the personal data are being processed. The GDPR states that: "*consent shall cover all processing operations carried out for the same or more purposes. Where processing has multiple purposes, consent shall be required for all processing operations for the same or more purposes*".
Informed consent is also linked to the idea of transparency since data subjects can be said to be informed only when a person has a real opportunity to know the processing features, i.e., when the information provided is detailed but also specific and understandable. The principle of transparency requires that any information sent to the public or data subjects should be concise, accessible, and understandable and should use clear and easy-to-understand language and, where appropriate, visual images. Such information may be provided electronically as delivered to the public via a website.
On the other hand, the complexity of online behavioral advertising technology makes it difficult for personal data subjects to identify the data controller and its purposes. If one tries to read any particular application's privacy policy, the third parties who may receive personal data often need to be named. If third parties are listed, consumers must read the privacy policies of these third parties to understand how the third parties may use the data. These third parties may be sharing the data with their third-party partners. In practice, consumers need an overview of the content and location of their data that may be transmitted or how it is used, even from a single application. The system behind even the most basic-seeming transaction can include hundreds of third parties, all with their purposes and policies regarding data handling.

A company may process personal data for online behavioral advertising when the data subject has given "*explicit consent*."[114] The Working Group and several experts agree that the only basis for legitimizing the

---

[111] Information Commissioner's Office (2017), *Consultation: GDPR Consent Guidance*, p. 21-22, https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

[112] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Paragraph 42, https://gdpr-info.eu/

[113] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 13, https://gdpr-info.eu/

[114] The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and the free movement of such data*, Article 7, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

processing of personal data is explicit consent [115]. The data subject can always withdraw his or her consent, and in such cases, the online behavioral advertising company must stop processing the data. Sensitive personal data such as medical data can only be processed for online behavioral advertising after the data subject has given "*explicit consent*." Member States can also choose not to allow the processing of sensitive data based on consent. Consent must be freely given, so consent given under pressure will not be valid. Since consent must be specific, consent to "*use personal data for commercial purposes*" will not be accepted. In line with the principle of transparency, consent must be informed. Companies should not hide relevant information in a footnote in their privacy policy. In principle, consent can be implied, but inaction rarely indicates a person's wishes. Case law from the European Court of Justice confirms that silence alone does not constitute consent. In most cases, companies can only lawfully process personal data after obtaining the data subject's explicit consent. Consent in data protection law can be seen as a tool to promote data subjects' control over their data.

Transparency is a prerequisite for data subjects to have some control over how online behavioral advertising companies use their data. Articles 10 and 11 of the GDPR require online behavioral advertising companies to provide at least information regarding their identity and processing purposes and provide additional information to ensure fair processing. Companies must always be transparent about processing personal data, regardless of whether they rely on consent. Internet users must be provided with additional information that is easy to read, and they must act affirmatively to give consent. These regulations have a significant impact on the way stakeholders present information online and ask for user consent. For example, companies will have to provide consumers with a table of contents containing the different purposes they want to process data and allow consumers to tick the boxes they want. On the other hand, agencies can place different banners, each asking for consent for each purpose for which the company wants to process data. One of the concerns of representatives of the online behavioral advertising industry is that such requirements will make browsing the Internet more frustrating because consumers have to deal with a new set of information.

3. EXPERIENCE FOR VIETNAM IN PROTECTING PERSONAL DATA

3.1. Vietnam context of online behavioral advertising

In Vietnam, in particular, and in the world in general, the ecosystem in the field of online behavioral advertising is still quite diverse, with most large companies and widespread networks becoming increasingly vital. From the consumer protection perspective, if there are few competitors in an area, consumers may be subject to less favorable conditions than the conditions under which they can switch from one provider to another. For the Draft Law on Personal Data Protection of Vietnam, an essential requirement is to meet the ability to prevent the binding of a data controller to ensure that consent is genuinely given freely, specifically, clearly, and clearly.[116] The Law on Personal Data Protection of Vietnam needs to ensure the adequacy of choices to form a prerequisite for the right to control personal data[117]. The lack of choice in cases of online behavioral advertising in Vietnam is understood in three different but closely related meanings.

---

[115] Traung P (2010), "EU Law on Spyware, Web Bugs, Cookies. Revisited: Article 5 of the Directive on Privacy and Electronic Communications", *Business Law Review*, 31(10), p. 216.

[116] The European Parliament (2016), *General Data Protection Regulation* (GDPR), Paragraph 42, https://gdpr-info.eu/

[117] Joseph Raz (1988), *The Morality of Freedom,* Publishing House. Oxford, p. 369.

One is a need for alternative services: In some of the most used online service areas, such as search engines and video streaming, a few service providers are the only dominant providers. In effect, Internet users have no other choice because the most essential features are only available on these services.

Second, the lack of alternative data processing models: While some "pay-as-you-go" or "freemium" (free + premium) business models are gaining popularity in some sectors[118], "free" services supported by online behavioral advertising remain the dominant trend in the Internet environment. For example, in the social media sector, large service providers are still primarily funded by online behavioral advertising revenue[119]. This means that although consumers can switch to another service, personal data is still processed similarly. In some homogeneous markets, the only viable business model, despite the coexistence of competing services, is to provide a free service but monetize the behavioral data of Internet users. Online behavioral advertising may not be technically necessary for most online services, but it is financially essential for operating such services. To promote diversity of choice, data controllers will provide Internet users with the option of payment in the form of money or other forms of consent-based payment for using personal data for online behavioral advertising purposes. This results in individuals who can afford to pay for do-not-track services enjoying a higher level of privacy than those who cannot afford to pay and, therefore, have no choice but to consent to the processing of personal data by the data controller.

Third, there is a need for alternative data networks. Once a data subject withdraws consent, the data controller is obliged to delete the relevant data immediately.[120] Unless there is another legal basis for processing or one of the exceptions applies [121]. At the same time, if the data has been provided to any third party and the data subject also requests that the third party delete it, the data controller must "*take reasonable steps, including technical measures*" to notify them of the request[122]. Notably, the data controller must ensure that withdrawing consent is as easy as giving consent[123]. This provision of the GPDR allows Internet users to switch from a service belonging to one online behavioral advertising network to another service belonging to a different network. However, if the two services are part of the same online behavioral advertising network, depending on the circumstances, switching between the two networks will make little, if any, difference. This is because

---

[118] Mark Sweney (2012), *Online Paid-content Market Poses Threat to Traditional Advertising, The Guardian,* https://www.theguardian.com/media/2012/nov/01/online-paid-contect-rise-8-billion- pounds. pounds

[119] Kurt Wagner (2017), *Pinterest Expects to Make More Than $500 Million in Revenue This Year*, https://www.cnbc.com/2017/03/21/pinterest-revenue-projected-at-500-million-this-year .html

[120]The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 17, Paragraph 1, Point b, https://gdpr-info.eu/

[121]The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 17, Paragraph 1, Point b, https://gdpr-info.eu/

[122]The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 17, Section 2, https://gdpr-info.eu/

[123]The European Parliament (2016), *General Data Protection Regulation* (GDPR), Article 17, Section 3, https://gdpr-info.eu/

by switching to a new service, Internet users are likely to have agreed to continue processing their data. In Google's case, unless a user terminates their account with all Google services (including Google Maps, YouTube, Gmail, etc.), simply switching from a third-party service to another service within Google's vast network will hardly reduce the amount of data Google holds about that Internet user. In 2012, Google announced a unified privacy policy update that would apply to all of Google's core services, allowing for the sharing of user profile data between services.[124] This left Internet users needing the option to separate their profiles across those services.

3.2. Policy recommendations for Vietnam

The 2013 Constitution of Vietnam affirmed the right of private privates to any ability to invade violation and opened a broad scope of rights private Are not only to any ability invade violation about body, house, and letter credit but still also the right to guard information about life living private honey person, secret honey family family. The Civil Code 2015, Law on Access to Information 2016, and Law on Children 2016 use the phrase "*information about private life, personal secrets, family secrets*" but do not define these concepts. According to the Ministry of Public Security statistics, Vietnam has 69 legal documents protecting personal data. However, the documents do not have a unified concept and content of personal data protection. There are more than ten terms related to personal information, including: "personal data," "personal information," "private information," "private information," "digital information," "personal information on the network environment," "private information," "information about private life," "family secrets," "inviolable right to privacy," "electronic database," "consumer information"... It can be seen that, in these terms, the term "personal information" is considered the most similar and closest to the term "personal data." In the system of legal documents in Vietnam, there are only 07 legal documents that define "personal information," the remaining documents mention the term "personal information " in the content of the regulations without explanation or referring to other legal documents.[125]

Although Decree No. 13/2023/ND-CP dated April 17, 2023 of the Government on personal data protection has defined "personal data" and "personal data protection", the scope of regulation of the Decree does not cover all areas and relationships of life and society, nor is it really compatible with the provisions on the right to privacy, personal secrets, and family secrets stated in the 2013 Constitution. Therefore, the requirement is to unify the term "personal data" to ensure consistency in content, scope, method, and specific cases of application.

On the other hand, according to Article 11, Decree 13/2023/ND-CP dated April 17, 2023, on personal data protection, the consent of the data subject is only valid when: (i) the data subject voluntarily and knows the contents of the type of personal data processed; the purpose of processing personal data; the organization or individual whose personal data is processed; the rights and obligations of the data subject. (ii) The data subject's consent must be clearly and specifically expressed in writing or voice by checking the consent box, using consent syntax via text message, selecting technical consent settings, or through another action demonstrating this. (iii) The consent must be conducted for the same purpose. When there are multiple

[124]Mark Milian (2012), *Google User Data to Be Merged Across All Sites Under Contentious Plan,* https://edition.cnn.com/2012/01/24/tech/web/google-privacy-policy/index.html

[125]Law on Cyber Security 2015; Law on Denunciation 2013, Decree No. 146/2018/ND-CP dated October 17, 2018, detailing and guiding measures to implement several articles of the Law on Health Insurance; Decree No. 85/2016/ND-CP on ensuring information system security at different levels; Decree No. 72/2013/ND-CP dated July 15, 2013, on management, provision and use of internet services and information on the network; Decree No. 52/2013/ND-CP dated May 16, 2013, on e-commerce; Decree No. 64/2007/ND-CP on the application of information technology in the activities of government agencies

purposes, the Personal Data Controller, the Personal Data Controller, and the Processor list the purposes for the data subject to agree to one or more stated purposes. (iv) The data subject's consent must be expressed in a format that can be printed or copied in writing, electronic, or verifiable format. (v) The silence or non-response of the data subject is not considered consent. For the provisions on consent to processing personal data, Vietnamese law can refer to the provisions of the GDPR on free, informed, specific, and unambiguous consent to supplement the wording explanation section of the draft Law on Personal Data Protection.

REFERENCES

1. Alan F. Westin (2015), *Privacy and Freedom,* Ig Publishing, p. 102-105.
2. Ashkan Soltani and Add (2009), Flash *Cookies and Privacy*, https://typeset.io/pdf/flash-cookies-and-privacy-3nekb4ffz4.pdf
3. Antoinette Rouvroy and Yves Poullet (2009), *Reinventing Data Protection?* , Springer Publishing, p. 51.
4. BJ Koops (2014), "The trouble with European data protection law", *International Data Privacy Law*, p. 251.
5. Castells, M. (2001), *The Internet Galaxy*, Oxford University Press, p. 27.
6. Carter Jernigan and Behram FT Mistree (2009), *Gaydar: Facebook Friendships Exposing Sexual Orientation*, https://firstmonday.org/ojs/index.php/fm/article/view/2611
7. Charles Fried (1968), "Privacy", *The Yale Law Journal*, p. 475, 482.
8. Claudia Quelle (2016), Privacy and Identity Management: Facing up to Next Steps, Publishing House. Springer, p.144;
9. Daniel J. Solove (2009), *Understanding Privacy,* Publishing House. Harvard University Press, p. 50.
10. Eoin Carolan (2016), "The continuing problems with online consent under the EU's emerging data protection principles," *Computer Law & Security Review*, 32(3), p. 462-473 The European Commission (2011), *Opinion 15/2011 on the definition of consent*, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
11. Eoin Carolan and Alessandro Spina (2015), *Nudge and the Law: A European Perspective,* Publishing House Hart Publishing, pp. 165–166.
12. Emily Bell, C.W. Anderson and Clay Shirky (2012), " Post-Industrial Journalism: Adapting to the Present," *Columbia Journal Review*, https://www.cjr.org/behind_the_news/post_industrial_journalism_ada.php
13. Frederik J Zuiderveen Borgesius (2017), "Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation," *European Data Protection Law Review*, 3(3), p. 360–361.
14. Gwenn Schurgin O'Keeffe, Kathleen Clarke-Pearson, and Council on Communications and Media (2011), "Clinical Report—The Impact of Social Media on Children, Adolescents, and Families," *Pediatrics*, 127(4), p. 800.
15. Gerald Dworkin (1988), *The Theory and Practice of Autonomy,* Publishing House. Cambridge University Press, p. 9.
16. Gloria González Fuster (2014), *The Emergence of Personal Data Protection as a Fundamental Right of the EU,* Springer, p. 254–257.
17. Helberger, N. (2016), *Digital Revolution: Challenges for Contract Law in Practice*, Hart Publishing, p 135–161.
18. Helen Nissenbaum (2009), *Privacy in Context: Technology, Policy, and the Integrity of Social Life,* Publishing House Stanford University Press, p. 140.
19. IAB Europe (2010), *Consumers Driving the Digital Uptake: The Economic Value of Online AdvertisingBased Services for Consumers* (2010), https://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf
20. Internet Advertising Bureau UK (2014), *The Data Deal: How Data-Driven Digital Advertising Benefits UK Citizens*, https://www.iabuk.com/policy/data-deal-how-data-driven-digital-advertising-benefits-uk -citizens

21. Information Commissioner's Office (2017), *Consultation: GDPR Consent Guidance*, p. 19-21, https://ico.org.uk/media/about-the-ico/consultations/2013610/gdpr-consent-guidance-consultation-form-word-201703.docx
22. Julie E. Cohen (2013), "What Privacy Is For", *Harvard Law Review*, 126(7), p. 1927-1932.
23. John Danaher (2016), "The Threat of Algocracy: Reality, Resistance and Accommodation", *Philosophy & Technology*, 29, p. 245.
24. Joseph Raz (1988), *The Morality of Freedom,* Publishing House. Oxford University Press, p. 369.
25. Joseph Raz (2009), *Between Authority and Interpretation: On the Theory of Law and Practical Reason,* Publishing House. Oxford University Press, p. 135.
Jiahong Chen (2018), "The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle," *European Data Protection Law Review*, 4, p. 36.

26. Kurt Wagner (2017), *Pinterest Expects to Make More Than $500 Million in Revenue This Year*, https://www.cnbc.com/2017/03/21/pinterest-revenue-projected-at-500-million-this-year.html

27. Kim McNamara (2011), "The Paparazzi Industry and New Media: The Evolving
28. OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, https://www.oecd-ilibrary.org/science-and-technology/oecd-guidelines-on-the-protection-of-privacy -and-transborder-flows-of-personal-data_9789264196391-en
29. Moerel L (2012), *Binding Corporate Rules: Corporate Self-regulation of Global Data Transfers, Dai University of Tilburg, p. 72.*
30. Mark Sweney (2012), *Online Paid-content Market Poses Threat to Traditional Advertising, The Guardian, https://www.theguardian.com/media/2012/nov/01/online-paid-contect-rise-8-billion-pounds*
31. Mark Milian (2012), *Google User Data to Be Merged Across All Sites Under Contentious Plan*, https://edition.cnn.com/2012/01/24/tech/web/google-privacy-policy/index.html
32. Monu Bedi (2016), "The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-up," *Northwestern University Law Review*, 110(2), p. 507.
33. Michael Barbaro and Tom Zeller Jr. (2006), "A Face Is Exposed for AOL Searcher No. 4417749", *The New York Times, https://www.nytimes.com/2006/08/09/technology/09aol.html*
34. Mireille Hildebrandt (2009), *Profiling and the rule of law*, Publishing House. Springer, p. 36.
35. NE Simmonds (1981), "Property, Autonomy, and Welfare," *ARSP*, 67(1), p. 61, 66.
36. NA Moreham (2006), "Privacy in Public Places," *Cambridge Law Journal*, p. 606.
37. Omer Tene and Christopher Wolf (2013), "Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent," *Information Security & Privacy News*, p. 19-28.
38. Omer Tene and Jules Polonetsky (2012), "To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising," *Minnesota Journal of Law, Science & Technology*, 13, p. 281.
39. Orla Lynskey (2014), "Deconstructing Data Protection: The Added-value" of a Right to Data Protection in the EU Legal Order," *International and Comparative Law Quarterly,* 63 (3), p. 569–597.

40. Philipp Hacker (2017), "Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things," *International Data Privacy Law*, 7(4), p. 26;

41. Production and Consumption of Celebrity News and Gossip Websites", *International Journal of Cultural Studies*, 14(5), 515.
42. Paul Ohm (2010), "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, 57, 1746-1748.
43. Paul M. Schwartz (1999), " Privacy and Democracy in Cyberspace," *Vanderbilt Law Review*, 52, p. 1607.

44. Portuguese Assembly (1976), The Constitution of Portugal, https://www.constituteproject.org/constitution/Portugal_2005
45. Ronald J. Krotoszynski, Jr. (2016), *Privacy Revisited: A Global Perspective on the Right to Be Left Alone*, Publishing House Oxford University Press, page 5.
46. Rishab Nithyanand and add (2016), *Adblocking and Counter-Blocking: A Slice of the Arms Race*, https://www.usenix.org/system/files/conference/foci16/foci16-paper-nithyanand.pdf
47. Richard A. Posner (1978), "The Right of Privacy", *Georgia Law Review*, 12(3), p. 397.
48. SI Benn (1976), "Freedom, Autonomy and the Concept of a Person", *Proceedings of the Aristotelian Society*, 76(1), p. 124.
49. Steven Levy (2011), *In the Plex: How Google Thinks, Works, and Shapes Our Lives*, Publisher Simon & Schuster, p. 3.
50. Scott Cleland (2011), *Search & Destroy: Why You Can't Trust Google Inc*, Publisher Telescope Books, p. 20.
51. Samuel D. Warren and Louis D. Brandeis (1890), "The Right to Privacy," *Harvard Law Review*, 04, p. 193.
52. The European Parliament (2012), Proposal on the protection of individuals about the processing of personal data and the free movement of such data (General et al.), p. 85, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011
53. The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and the free movement of such data*, Article 2, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046
54. The European Parliament (2016), *General Data Protection Regulation* (GDPR), Paragraph 32, https://gdpr-info.eu/
55. The European Commission (2017), *Guidelines on Automated Individual decision-making and Profiling for Regulation 2016/679*, p. 10, https://ec.europa.eu/newsroom/article29/items/612053
56. The European Commission (2011), *Opinion 15/2011 on the definition of consent*, retrieved access in https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
57. T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt (2021), *Data Protection: CJEU case law review – 1995-2020*, https://www.dpcuria.eu/case-law-review-1995- 2020.pdf
58. The CJEU Second Chamber (2019), *Fashion ID GmbH & Co. KGVerbraucherzentrale NRW eV* , https://www.5rb.com/case/fashion-id-gmbh-co-kg-v-verbraucherzentrale-nrw-ev/
59. Traung P (2010), "EU Law on Spyware, Web Bugs, Cookies, etc. Revisited: Article 5 of the Directive on Privacy and Electronic Communications", *Business Law Review*, 31(10), p. 216.
60. The Fed er al Con sti tu tion al Court (1965), *BVerfGE 65, 1 [1965] s II. 1. A* , https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/12/rs19991215_1bvr065396en.html
61. The European Parliament (1995), *Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, on the protection of individuals about the processing of personal data and the free movement of such data*, https:/ /eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046.
62. The European Parliament (2016), *Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons about the processing of personal data and the free movement of such data, and repealing Directive 95 /46/EC (General et al.) (Text with EEA relevance)*, https://eur-lex.europa.eu/eli/reg/2016/679/oj
63. The European Commission (2018), Consumer market study on online market segmentation through personalized pricing/offers in the European Union, https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalized-pricingoffers-european-union_en

64. The Fed er al Con sti tu tion al Court (1965), *BVerfGE 65, 1 [1965] s II. 1.* A , https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1999/12/rs19991215_1bvr065396en.html
65. Woodrow Hartzog (2018), *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Publishing House. Harvard University Press, p. 118–119.
66. William L. Prosser (1960), "Privacy", *California Law Review*, 08, p. 383.

67. Zuboff Shoshana (2015), "Big Other: surveillance capitalism and the prospects of an
68. Zuiderveen Borgesius Frederik (2016), "Singling out people without knowing their names – Behavioral targeting, pseudonymous data, and the new Data Protection Regulation," *Computer Law & Security Review*, 32(2), p. 256–271.