13th International Scientific Conference "Employment, Education and Entrepreneurship"

Conference Proceedings

FACTORS INFLUENCING THE ETHICAL AND LEGAL CHARACTER OF DIGITAL MARKETING

Biljana Knežević[1]
Marija Bešlin Feruh[2]
Maja Cogoljević[3]

DOI: 10.5937/EEE24032K
JEL: K00, K24, M31
Review Scientific Paper

ABSTRACT

This paper explores the evolving legal and ethical landscape of digital marketing, highlighting significant regulatory gaps and the emergence of new entities and norms. It identifies a new type of legal entity—the virtual stakeholder—that intrudes on consumer privacy through tracking systems, operating independently of traditional legal frameworks. The rise of "community guidelines" as autonomous, supranational laws illustrates a shift from state-centered legal systems to policy-driven regulations imposed by global digital platforms. The paper underscores the inadequacy of existing regulations, such as the General Data Protection Regulation and national laws, in addressing modern digital marketing practices and international challenges. The erosion of state sovereignty over digital commerce and the slow adaptation of classical laws to technological advancements are noted, alongside the extensive use of the Internet by consumers and businesses, raising ethical concerns. Concslusions include developing specific legal frameworks, regulating community guidelines, and advancing regulatory technology. This approach aims to align legal standards with the rapid changes in the digital environment, ensuring greater protection and fairness for users and businesses alike.

KEYWORDS

digital marketing, consumer, law, ethics, privacy and data protection

INTRODUCTION

Contemporary scientific literature addressing the ethical and legal dimensions of internet-based business thoroughly examines several critical aspects of digital marketing. There is a broad consensus within the academic community that this field remains underexplored, as key concepts associated with collective social responsibility and its legal and ethical implications remain inadequately regulated. This assertion is supported by the current deficiency in legislation aimed at ensuring the seamless conduct of digitized transactions in everyday business practices. Such regulatory gaps prompt concerns within both business and academic circles regarding consumer protection and potential societal harm.

[1] Higher Business School of Vocational Studies Cacak, Beograd, Srbija, knezevicbilja@gmail.com, ORCID: 0009-0000-3659-5569
[2] Higher Business School of Vocational Studies Cacak, Beograd, Srbija, marijabf@gmail.com, ORCID: 0000-0001-5172-8331
[3] Faculty of Business Economics and Entrepreneurship, Belgrade, Serbia, maja.cogoljevic@vspep.edu.rs, ORCID: 0000-0002-5766-9325

The objective of this paper is to delineate the legal and ethical dimensions of digital marketing, encompassing the primary stakeholders engaged in the digital domain. The research, conducted in 2024, includes a review of domestic and international regulatory frameworks, secondary data analysis, notable academic perspectives, and evaluations by state authorities and experts, along with stakeholder positions in the marketing sector. The study incorporates data critical for mitigating risks associated with unfair business practices, deviations from established business ethics (*ex fide bona*), and the safeguarding of consumer data.

RESULTS AND DISCUSSIONS

The findings indicate a significant lack of regulation and inadequacies in business relations within this domain, compounded by partial deficiencies in stakeholder competence and societal awareness. There is a notable absence of understanding regarding digital ethics, particularly concerning privacy and personal data protection, as well as intellectual property rights. Over the past decade, the digital economy has evolved from static web pages to dynamic, cloud-based web applications. Internet users have increasingly engaged with these platforms as content creators, entrepreneurs, or consumers, participating in a "many-to-many dialogue" where communication is bidirectional and pervasive.

The Internet business ecosystem has developed highly dynamic communication platforms, integrating social media with business operations, and frequently interacting with consumers. This has enabled companies to tailor and promote their products in alignment with consumer behaviors and needs, fostering what is often termed "personalized marketing."

Modern enterprises employ sophisticated techniques to gather information about customers that would be otherwise inaccessible offline. These methods include various forms of communication, anonymous tracking, and extensive data dissemination (Sipior et al., 2024). During online transactions, customers may be prompted to provide personal data through website registration, membership applications, surveys, contests, or other interactions that solicit personal information. Consumers often believe this information is collected solely for the immediate transaction, which may not always be the case. This is particularly relevant for search engines, which may, through email or instant messaging, involve third parties in data collection without explicit consent (Ibidem). The monitoring of internet users has been facilitated by technologies such as "clickstream" tracking, including cookies, web bugs, and other methods that identify customer behavior patterns covertly (Id). Attention is also drawn to emerging applications of artificial intelligence, including machine learning systems and automated integrated applications (Knežević, Bešlin Feruh, 2024).

Despite the perception that legislative measures have addressed issues related to digital privacy, advertisers frequently evade repercussions for infringing upon client privacy. Commonly, websites involved in marketing activities display notifications such as "This website uses cookies," offering visitors a binary choice: to accept "only necessary cookies" or to accept all cookies. However, this practice, which ostensibly complies with global legislation—including that of the European Union and the Republic of Serbia – often fails to ensure genuine protection of personal data in practice. For instance, regardless of the choice made, whether accepting all cookies or only necessary ones, tracking of the user is typically continuous. Furthermore, the term "necessary cookies" remains undefined, leading to ambiguity and potential misuse. Additionally, tracking techniques such as click-streaming continuously monitor consumer activity across the internet.

In the European Union, the primary legislative framework governing digital marketing is the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council, dated 14

September 2022). This regulation aims to establish foundational legal norms and principles to promote fair and unobstructed digital business practices. The Digital Markets Act introduces criteria for identifying "gatekeepers," which include major digital platforms providing online search engines, app stores, and internet messaging services. These gatekeepers are mandated to uphold fair business practices and ensure competitive market conditions. Additionally, their ability to oversee the entire buying and selling process on their platforms effectively positions them as supervisory entities, potentially assuming roles akin to regulatory authorities within their own ecosystems.

The Digital Markets Act seeks to counteract such supervisory tendencies by prescribing specific general provisions for digital business operations. However, the obligations for stakeholders to comply with this act will only come into effect in March 2024, allowing a period for practical implementation and adaptation.

The Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council, dated 19 October 2022) addresses intermediary entities such as online marketplaces, social networks, content-sharing platforms, app stores, and platforms involved in online travel and accommodation bookings. The primary objectives of this regulation are to prevent illegal and harmful activities, mitigate the spread of misinformation, ensure user security and the protection of fundamental rights, and establish transparency across online platforms.

The Digital Services Act specifically prohibits targeted advertising aimed at children and sets forth procedures for reporting harmful online content. It also delineates requirements for network infrastructure to safeguard consumers, including data about internet service providers, registered domains, domain names, hosting services (both cloud-based and traditional web hosting), and platforms that facilitate transactions between buyers and sellers (e.g., websites, app stores, and social media platforms).

In contrast to the Digital Markets Act, the Digital Services Act became effective on 17 February 2024, mandating compliance across all platforms. As of September 2024, the regulation has been applied to over 45 million users within the European Union and is enforced on large online platforms and widely used search engines. However, its practical implementation has thus far reached only 10% of the European population. The European Commission, in collaboration with national authorities, is responsible for enforcing this act. The specifics of how each member state will ensure compliance and the methodologies for monitoring adherence to this supranational regulation remain ambiguous.

In the European Union, a significant force behind the adoption of legal measures by the European Commission is the European Court of Justice, which interacts directly with both digital content creators and consumers through its jurisprudence and rulings. For instance, the Court's decision in Case C-371/20 (Peek, Cloppenburg, 2022) underscored the necessity for digital content creators to clearly disclose when their content constitutes advertising. This ruling influenced the adoption of the Unfair Commercial Practices Directive (Directive 2005/29/EC), which aims to enhance transparency and protect consumers from misleading marketing practices (Bormane, Urbane, 2023).

Despite these efforts, the EU has yet to establish a fully integrated and clearly regulated legal framework for monitoring consumer behavior that would ensure comprehensive enforcement of existing regulations. Currently, approximately 90% of consumers are subject to the regulations of major stakeholders, or "intermediary entities," as defined by the Digital Services Act. These intermediary entities often retain the autonomy to self-regulate, effectively creating parallel legal and ethical norms that may diverge from national and EU standards. This autonomy permits internet stakeholders to adopt ethical practices that can be inconsistent, varying from one country to another or between different entities. Consequently, internet companies may operate with ambiguous ethical standards.

This issue is particularly pertinent in the context of the European Open Internet Access Regulation (Regulation 2015/2120), which has been in effect since 2016 as part of the EU Digital Strategy. This regulation safeguards end users' access to online content and services by prohibiting any form of discrimination or restriction, such as blocking or throttling, by internet service providers. While this regulation promotes broad internet access rights, it does not fully address the need for precise legal provisions to protect users comprehensively, including those using marketing services.

The current legal framework for direct marketing within the European Union is governed by general regulations that do not explicitly address internet-based practices. Regulation (EU) 2016/679, commonly known as the General Data Protection Regulation, provides broad data protection guidelines but does not specifically target internet marketing practices. The proposed regulation for ePrivacy (Proposal for an ePrivacy Regulation, January 10, 2017) has been under consideration by the Council of Europe for nearly six years and is still pending discussion by the European Parliament, with no clear timeline for its adoption.

In the interim, the European Commission has drafted a Directive on Privacy and Electronic Communications (2002/58/EC), which also remains unadopted by the European Parliament. The ePrivacy Regulation is intended to serve as a "lex specialis" relative to the GDPR. Following the legal principle of *lex specialis derogat legi generali*, this regulation aims to address specific technical developments and widespread phenomena in digital communication more comprehensively. It seeks to ensure a uniform level of protection for all users engaging with electronic communication services.

The ePrivacy Regulation is designed to apply first to electronic communication service providers such as WhatsApp, Facebook Messenger, and Skype, and then to metadata—data that describes secondary information, including the origin, creation date, or location of primary data. The regulation proposes that private data should only be retained if necessary for billing and payment purposes. Furthermore, it seeks to address contemporary marketing challenges by introducing precise legal standards for tracking technologies, such as cookies. This proposal would grant users the explicit right to accept or decline tracking and provide protections against unsolicited communications, including spam emails, SMS, and automated calls. Additionally, the proposal suggests that oversight of these regulations should fall under the same authorities responsible for enforcing the General Data Protection Regulation.

The current protection of personal data for EU citizens is primarily governed by the General Data Protection Regulation, a comprehensive framework that applies universally across the European Union. The General Data Protection Regulation serves as a broad legislative measure for personal data protection, encompassing all EU citizens regardless of their internet usage. However, this regulation functions as a generic rule and does not address the specificities of internet-based practices and direct marketing.

This general approach proves insufficient in the context of direct marketing and online behavior, particularly given that EU citizens are often targeted by marketing activities originating from outside the EU (e.g., from the United States or the United Kingdom), which may not be subject to EU regulations. A more pressing issue is that the GDPR, which was proposed eight years ago, has become outdated in addressing contemporary marketing practices. The regulation primarily addresses older forms of direct marketing such as email, spam, and cookies, while failing to account for newer, more intrusive tools that have emerged, including neuromarketing techniques, echo chambers, and various applications of artificial intelligence.

These advanced methods pose significant challenges that the current regulatory framework does not adequately address, highlighting the need for updated and more specific regulations to effectively protect EU citizens from evolving marketing strategies and technologies.

In the Republic of Serbia, the overarching legal framework for data protection and digital marketing is primarily governed by the Personal Data Protection Act (Official Gazette of RS, No. 87/2018). In addition to this foundational legislation, several other laws contribute to the regulation of electronic and digital communications:

- Law on Electronic Commerce (Official Gazette of the RS, Nos. 41/2009, 95/2013, 52/2019),
- Law on Electronic Communications (Official Gazette of the RS, Nos. 44/2010, 60/2013, 62/2014, 95/2018, 35/2023),
- Law on Information Security (Official Gazette of RS, Nos. 6/2016, 94/2017, 77/2019),
- Law on Advertising (Official Gazette of RS, Nos. 6/2016, 52/2019).

Furthermore, the Serbian government has implemented strategic initiatives related to internet business through:

- Strategy for the Development of the Information Society and Information Security (2021-2026),
- Strategy for the Development of the Electronic Communications System (up to 2027).

Marketing practices in the digital environment are also addressed within the Criminal Code (Official Gazette of RS, Nos. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019). This code stipulates penalties for various cybercrimes, including: A prison sentence of up to two years for the creation and introduction of malware into another person's computer, contingent on the extent of damage caused; Fraud committed via the internet, which is treated as a distinct offense, punishable by up to ten years in prison if the financial damage exceeds a specified threshold; Unauthorized access to another person's computer, network, or electronic data processing, which incurs a prison sentence ranging from six months to three years.

These regulations collectively aim to address the complexities of digital marketing and electronic communication, though they may still face challenges in fully aligning with the rapidly evolving nature of digital technologies and marketing practices.

It is evident that while certain legal provisions prohibit specific acts, their applicability to digital marketing and consumer monitoring on the internet remains indirect and problematic. For instance, it is debatable whether cookies or spam can be classified as viruses, or how unauthorized access to computers and internet fraud should be defined within the context of digital marketing. The Criminal Code of the Republic of Serbia, for instance, addresses offenses primarily related to hardware systems, such as computers and computer networks. However, contemporary digital challenges predominantly involve software regulation, as the internet is accessed through a variety of devices, including smartphones, tablets, and other Wi-Fi-enabled gadgets.

These regulatory challenges mirror those faced by many EU countries, where a general legal framework, such as the General Data Protection Regulation in the EU and the Law on the Protection of Personal Rights in Serbia, governs personal data protection. Both frameworks offer broad protection for personal data but do not specifically address the nuances of internet-based marketing or emerging digital tools.

In Serbia, as in other jurisdictions, issues such as cross-border direct marketing and outdated regulations regarding modern technological tools remain inadequately addressed. This regulatory gap underscores a critical issue: in the absence of specific state and legal norms, the behavior of internet users is often governed by multinational corporations, or "intermediary entities," which can create their own regulatory frameworks.

These issues are significant not only for users and consumers within the EU and Serbia but also on a global scale, given the internet's universal reach. The widespread use of the internet by businesses is illustrated in Figure 1.

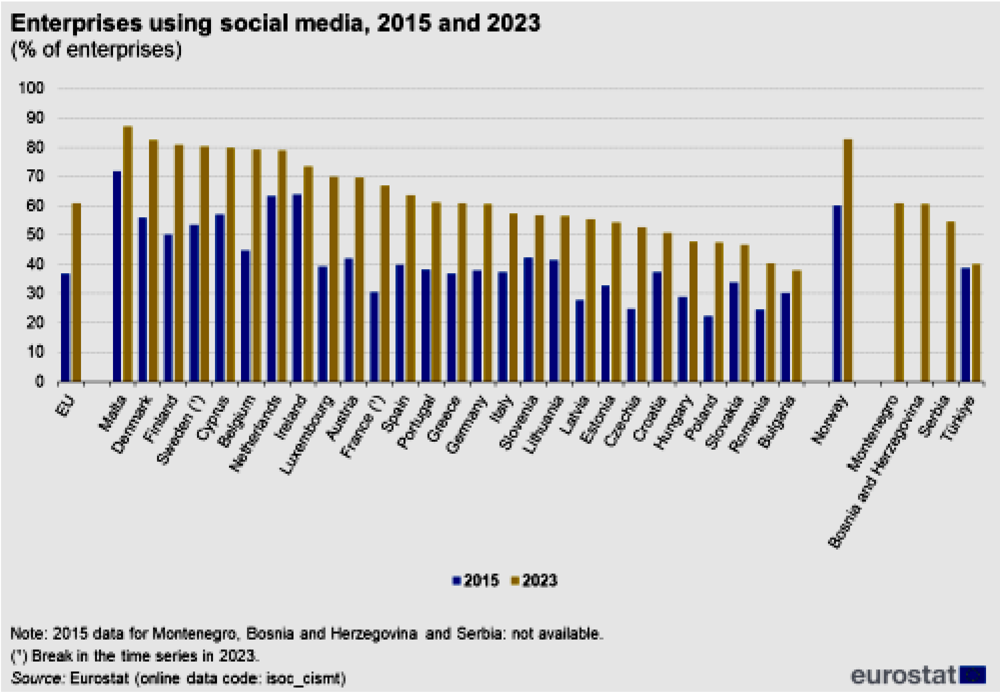

Figure 1. Enterprises uses social media 2015 and 2023
Source: Eurostat (online data code: isoc_cismt

In 2023, 60.9 % of EU enterprises used at least one of these types of social media, an increase by 24.1 percentage points compared to 2015. Percentages do vary widely from country to country, ranging from 80 % and more in Malta 87.1 %, Denmark 82.5 %, Finland 81 % and Sweden 80.3 % to less than 45 % in Romania 40.5 % and Bulgaria 38 % (The European Comission, 2023).

In EU 60.9 % enterprises used social media in 2023. More than 8 in 10 large enterprises (86 %) reported using social media, a share significantly higher than the one recorded for small enterprises (58 %). It is noticeable that 29.5 % of enterprises in the EU used only one of the three types of social media and another 23.3 % used two types of social media. 8.1 % of enterprises reported using 3 types of social media. Almost one third of small enterprises, 29.5 % preferred to concentrate on the use of one type of social media compared to slightly less than one-fourth i.e. 23.3 % using two and 6.4 % using three types of social media. On the contrary, the shares of EU large enterprises using two and three types of social media 31.7 % and respectively 29.8 % were higher than the percentage using only one type 24.5 % (The European Comission 2023).

Data indicates that in highly developed nations, approximately 80% of entrepreneurial activities are conducted over the internet. In the context of inadequate or weak regulation, users and consumers increasingly engage in transactions where they are vulnerable to unfair practices by advertisers and principal stakeholders online. Many companies have established their own oversight mechanisms, such as fact-checking systems, which involve filtering information and intersect with fundamental constitutional rights, including freedom of information, freedom of speech, and freedom of belief and religious views.

Given that a significant number of consumers now spend more time engaged in virtual rather than physical shopping, the prevailing thesis is that users, when participating in various online activities (such as freelancing, influencing, drop shipping, affiliate marketing, and shopping), are more likely to be governed by the "legislation" of multinational corporations rather than by the laws of individual countries. This is evidenced by the data presented in Figure 1.

This "legislation," often referred to as community guidelines, encompasses a broad array of practices that are rarely addressed by national regulations. These practices include the use of cookies, web tracking, email tracking, and instant message tracking. Additionally, this "regulation" often involves ethically questionable practices, notably neuromarketing, which employs psychological and neurological techniques, sometimes without explicit user consent. Neuromarketing strategies leverage emotional responses, motivation, and perception to influence consumer behavior (Alsharif et al., 2023).

The susceptibility of consumers to varying ethical standards among stakeholders is exemplified by the case of DoubleClick Inc., as described by Charters. DoubleClick, a prominent advertising company specializing in the creation of internet banners (pop-ups), plays a crucial role in the advertising ecosystem by monitoring user behavior and internet trends to tailor advertisements according to user interests. Acting as an intermediary between advertisers and end users, DoubleClick not only facilitated targeted advertising but also refined data profiles of individuals and companies, leveraging proprietary databases.

In response to concerns raised by the Electronic Privacy Information Center (EPIC), which advocates for privacy rights, DoubleClick's practices were scrutinized for their potential negative implications for user privacy. The public backlash following EPIC's critique was swift and intense, compelling DoubleClick to alter its proposed practices (Charters, 2022).

Despite the criticism, DoubleClick's CEO defended the company's actions, asserting that, from an ethical standpoint, the company had not acted inappropriately. He argued that DoubleClick was ahead of its time and had anticipated that users would eventually accept such practices. The study concludes that there may be an ethical rationale for DoubleClick's electronic monitoring practices if users are given a clear choice to accept or reject such tracking. According to Kantian ethics, such an invasion of privacy could be justified if it respects user autonomy and informed consent (Ibidem).

The DoubleClick case underscores the frequent exposure of users and consumers to ethically dubious practices within the digital marketing sphere. This case highlights a broader issue: both legal theorists and ethicists acknowledge that consumers often lack sufficient knowledge to safeguard their personal rights online. Moreover, there is a discernible gap in the legal and ethical understanding among modern technological elites, leading to potential misuse of advanced technological tools.

The study reveals that DoubleClick's founder appeared to have deliberately engaged in practices that infringed upon consumer rights, operating under the presumption of tacit consent. This presumption reflects a broader issue where technological advancements outpace legal frameworks, resulting in regulatory lag. In this context, the law – traditionally understood as a state-based regulatory mechanism – emerges as a "slow form of regulation" that struggles to keep pace with rapid technological development.

The pervasive use of tracking systems on the internet, including cookies on virtually every website and extensive databases managed by search engines, complicates the enforcement of comprehensive regulatory measures. This situation illustrates a shift from a simple binary relationship of seller-consumer or seller-consumer-state to a more complex dynamic involving digital multinational companies and platforms. These entities, whether acting as advertisers or search engines, have increasingly assumed pivotal roles in regulating digital interactions.

The contemporary landscape of digital business reveals a significant shift from the 20th-century liberalism, which was grounded in Locke's theory of the inviolability of private property and the clear demarcation between individual ownership and external claims. At the dawn of the 21st century, these principles have been increasingly overshadowed by a pragmatic approach driven by technological advancement. This shift prioritizes technological efficacy over abstract concepts such as individual freedom, justice, and equality.

The prevailing focus on "practicality," a term that remains inadequately defined in the context of emerging technologies, suggests a reconfiguration of traditional legal and ethical standards. The concept of diverse, autonomous sources of law on the internet aligns with modern theories of freedom as non-domination. This theory, rooted in political and legal pluralism, posits the existence of multiple centers of power and a spectrum of ethical principles that are interpreted contextually rather than universally. This evolving paradigm reflects a move towards a more fragmented and dynamic regulatory environment where traditional notions of individual rights and justice are continually renegotiated in response to technological developments (Zanitelli, 2022).

CONCLUSION

This study has identified several intricate factors influencing the legal and ethical dimensions of digital marketing:

1. Emergence of Virtual Stakeholders: A novel legal entity has emerged in the seller-consumer dynamic: the virtual stakeholder. This entity, through tracking systems, unlawfully collects consumer data, infringing on constitutional privacy rights. It acts as an intermediary in all interactions during the buying and selling process. This intermediary not only influences the transaction but also plays a role in standardizing the process according to its own autonomous ethical principles. This creates a new form of law that has yet to be thoroughly integrated into legal theory.
2. Formation of Community Guidelines: A new form of legal norm, termed "community guidelines" or usage policies, has developed. These guidelines regulate the interactions between sellers, consumers, and advertisers but do not fit within the formal hierarchy of legal acts within any country. They are part of the policy framework of virtual stakeholders and can be viewed as a type of autonomous, supranational law. This represents a historical singularity in legal regulation, forming a parallel system to traditional legal norms.
3. State Sovereignty and Regulatory Challenges: The lack of sovereign regulation governing online transactions and advertising compounds the complexity of the digital marketing environment. The erosion of national authority over this global phenomenon is evident, as the Internet has become a domain largely governed by ambiguous global rules. This shift highlights the inadequacy of traditional legal mechanisms, which struggle to keep pace with the rapid technological advancements and the transnational nature of the Internet. Regulatory bodies face challenges due to insufficient tools, competencies, and technological expertise, making classical legal frameworks appear outdated and slow.
4. Massive Internet Utilization: The extensive use of the Internet by both consumers and entrepreneurs, despite concerns about legal and personal security, underscores an ethical precedent that warrants further sociological and psychological investigation. This widespread adoption of the Internet has shifted economic activities to a global platform, often outside the effective reach of state regulation, highlighting the need for more robust and adaptive regulatory approaches.

REFERENCES

Alsharif, A.H., Salleh, N.Z.M., Abdullah, M., Khraiwish, A., Ashaari, A. (2023). Neuromarketing Tools Used in the Marketing Mix: A Systematic Literature and Future Research Agenda. Sage Open, 13(1). https://www.researchgate.net/publication/369028665NeuromarketingToolsUsedintheMarketingMixASystematicLiterature and Future Research Agenda

Bormane, S., Urbane, M. (2023). The factors influencing legal and ethical digital marketing communication. 24th International Scientific Conference "Economic Science for Rural Development", Proceedings, pp. 188-196.

Charters, D. (2002). Electronic Monitoring and Privacy Issues in Business-Marketing: The Ethics of the DoubleClick Experience. Journal of Business Ethics, 35, 243–254.

Court's decision in Case C-371/20 (Peek, Cloppenburg, 2022).

Criminal Code ("Official Gazette of RS", 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019).

Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

Digital Services Act Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

Directive on Privacy and Electronic Communications (2002/58/EC).

Knežević, B., Bešlin Feruh, M. (2024). Ethical and legal aspects of using artificial intelligence in marketing. In V. Kuleto (Ed.), Book of Extended Abstracts: 2nd LINK IT & EdTech International Scientific Conference – LINK IT&EdTech24. Belgrade, Faculty of Contemporary Arts, Information Technology School.

Law on Advertising ("Official Gazette of RS", 6/2016, 52/2019).

Law on Electronic Commerce ("Official Gazette of RS", 41/2009, 95/2013, 52/2019).

Law on Electronic Communications ("Official Gazette of RS" 44/2010, 60/2013, 62/2014, 95/2018, 35/2023).

Law on Information Security ("Official Gazette of RS", 6/2016, 94/2017, 77/2019).

Law on Protection of Personal Data ("Official Gazette of RS, 87/2018).

Open Internet Access (Regulation EU 2015/2120).

Proposal for a Regulation of the European Parliament and of the Council (EU January 10, 2017).

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Sipior, J.C., Ward, B.T., Rongione, N.M. (2024). Ethics of Collecting and Using Consumer Internet Data. Information Systems Management, 21(1), 58–66.

Strategy for the Development of Information Society and Information Security or the Republic of Serbia from 2021 to 2026.

Strategy for the Development of the Electronic Communication system of the Republic of Serbia until 2027.

Zanitelli, M. (2022). Freedom as Non-Domination and Private Law's Autonomy. Law, Ethics and Philosophy, 9, 47-63.

Internet sources:

https://commission.europa.eu/law/law-topic/consumer-protection-law/consumer-contract-law_en

https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en

https://digital-strategy.ec.europa.eu/en/policies/safer-online