JLP JOURNAL OF LAW AND POLITICS

Data Safety Rights in Usage of Digital Platforms

Hana Tiro

©Author(s)

DOI: https://doi.org//10.69648/CAHT8406

Journal of Law and Politics (JLP), 2026; 7(2), 101-110.

jlp.ibupress.com

Online ISSN: 2671-3438

Application: 14.08.2026

Revision: 20.09.2026

Acceptance: 22.10.2026

Publication: 26.10.2026

Tiro, H. (2026). Data safety rights in usage of digital platforms. Journal of Law and Politics, 7(2), 101-110. https://doi.org//10.69648/CAHT8406

Hana Tiro

Independent researcher, Sarajevo, Bosnia and Herzegovina

https://orcid.org/0009-0007-7430-6837

Correspondence concerning this article should be addressed to Hana Tiro,

Email: hanatiro@outlook.com

BUP BALKAN UNIVERSITY PRESS

Abstract

This paper explores the intersection of user's rights and online activities in the context of everyday use of digital tools. It examines the role of digital platforms, their vulnerabilities, and the types of information processed in daily internet usage, and explores how personal information is shared online. Discussion focuses on the implications of users' knowledge of data privacy law, best practices for safeguarding information, protecting personal data, and understanding how data circulates within digital environments. Examples are drawn from popular social media platforms and online shopping websites, showing the users' experiences with data security. The paper explores how human rights can be integrated into cybersecurity frameworks and how laws can be implemented in the context of daily internet use, examined with a focus on individual persons as the center of cybersecurity laws. It addresses the needs and concerns of average internet users around their daily interactions and challenges they face in maintaining security and privacy online.

Keywords: Cybersecurity, personal data, online payments, privacy rights, digital rights

Data Safety Rights in Usage of Digital Tools

Digital tools have significantly impacted daily life, including socializing, shopping, learning, and entertainment. They facilitate communication, financial activities, and personal data exchange across platforms like Facebook, Instagram, and TikTok, while also integrating personalized recommendations and cloud-based data storage (Barykin et al., 2020). This digital ecosystem also comes with significant risks related to privacy, data security, and the potential for exploitation of personal information.

This paper explores the relationship between human rights, data security, and digital platforms, focusing on user rights in Europe and the Western Balkans. It discusses current legislation and the need for global cooperation to enforce privacy laws and prevent digital rights abuses, and in that way reducing the risks of cyber threats.

The referenced literature provides a comprehensive foundation for understanding digital commerce, data protection, and cybersecurity governance. Economics of Digital Ecosystems examines the economic structures of digital ecosystems, highlighting their role in the contemporary digital market. The Electronic Commerce Law establishes the legal framework governing electronic transactions and online trade. Publications from the European Commission (2022, 2023) and the European Union (2019) outline key principles of digital regulation, consumer rights, and personal data protection within the European digital environment. Cybersecurity and Human Rights in the Western Balkans analyzes cybersecurity governance and its implications for human rights in the Western Balkans region. Finally, Protection of Personal Data in the Context of E-Commerce explores privacy challenges in e-commerce and the importance of personal data protection, compliance, and consumer trust when it comes to online business operations.

The paper presents types of personal data that users share on digital platforms, potentially leading to identity theft, unauthorized surveillance, and privacy breaches. Cybersecurity encompasses the tools, practices, and policies to ensure that digital platforms are safe for use because data protection is a basis for individual freedom. Data privacy is a technical issue as much as a fundamental human right in the digital age.

Vulnerabilities and Data Processing in Everyday Internet Usage

Digital platforms collect data which can be categorized into personal data and transactional data. Personal data refers to information related to an identified or identifiable individual, including de-identified, encrypted, or pseudonym-data. This data falls under the General Data Protection Regulation (GDPR), the EU's main data protection law, and can be used to re-identify a person. Personal data includes names, addresses, email addresses, IP addresses, identification card numbers, cookie IDs, phone advertising identifiers, and data held by hospitals or doctors (European Commission, 2023). Transactional data is a collection of records in a database that record individual transactions, such as customer purchases or flight bookings. It includes transaction identity numbers and lists of items involved. Every interaction a user has with a digital platform, whether it's a social media post, an online purchase, or simply browsing a website, leaves behind a trace of data (ScienceDirect, n.d.). In legal and regulatory terms, this passage explains that digital platforms process two principal categories of data: personal data and transactional data, each carrying distinct legal implications. Personal data encompasses any information that directly or indirectly identifies a natural person, even data that has been encrypted, or under a pseudonym, or partially anonymized, may remain subject to legal protection if an individual can potentially be re-identified. Consequently, organizations collecting or processing personal data must comply with principles of lawfulness, transparency, purpose limitation, and data security. In contrast, transactional data may not always constitute personal data, yet it can still be subject to data protection laws when linked to an identifiable individual.

From a legal perspective, every user interaction with a digital platform generates data that may create obligations regarding privacy, data governance, cybersecurity, and regulatory compliance. Therefore, digital platforms must ensure that both personal and transactional data are collected, stored, processed, and shared in accordance with applicable legal standards. For example, social media platforms allow users to share vast amounts of personal information, often without fully realizing how much of their data is exposed to advertisers, hackers, or even other users. E-commerce sites like Amazon and eBay store transactional data, including payment information and shipping addresses, making them prime targets for cybercriminals. Similarly, mobile apps, particularly those that use location tracking features, collect data on users' whereabouts, preferences, and interactions, creating significant privacy concerns. These platforms may expose users to numerous

privacy risks due to their data collection practices, security vulnerabilities, and the potential for misuse of the data they handle.

Digital platforms continue to face threats from cybercriminals, despite improvements in cybersecurity. There are concerns about how third parties misuse personal data, as companies collect data directly from users (first-party data) and from various sources (third-party data). First-party data is seen as more trustworthy, but poor handling of personal data can result in privacy violations and fraud. Third-party data also poses risks, such as overlapping information and doubts about how it was collected (Morić et al., 2024). This data can be manipulated to influence consumer behavior, shaping political views, purchasing decisions, and even affecting a person's social environment. The lack of transparency in how this data is used or shared contributes to users' vulnerability and the erosion of their privacy.

Platforms' Responsibilities in Data Protection

Service providers such as social media companies, e-commerce platforms, or app developers have a responsibility to protect users' data under international human rights frameworks. Under the United Nations' Universal Declaration of Human Rights (UDHR), Article 12, individuals have the right to privacy and protection from arbitrary interference in their personal affairs. This means platforms must secure personal data against unauthorized access, misuse, or theft, and provide transparency to users about the data they collect and obtain informed consent before collecting sensitive information (United Nations, 1948). However, current regulatory structures are often inadequate, with many countries lacking comprehensive data privacy laws, leaving users vulnerable to exploitation. Additionally, enforcement of existing regulations can be inconsistent, with some companies exploiting loopholes to avoid accountability. The global nature of the internet further complicates matters, with data protection laws varying significantly across jurisdictions, creating challenges in enforcing data protection standards.

The circulation of data can create a web of surveillance that users are often unaware of. Websites use cookies and tracking technologies to collect user behavior information, but these can also collect and share personal data without explicit consent, contributing to privacy erosion. Personal data is often shared with third parties, who aggregate and resell it, raising privacy concerns. Cookies are small text files stored on a user's computer or mobile device, used by websites to optimize efficiency, track browsing habits, create user profiles, and display targeted online

advertising based on user preferences. Websites must obtain consent before installing cookies on a device, explain how cookie information will be used, and allow users to withdraw consent. Cookies used for communication transmission, such as load balancing, do not require consent. Cookies necessary for providing an online service, such as filling in online forms or using shopping baskets, do not require consent (European Union, 2019).

Laws and Regulations for Safeguarding User Rights in Digital Spaces

The General Data Protection Regulation (GDPR), which is an EU-drafted privacy and security law, mandates organizations to collect and target EU-related data. Effective May 25, 2018, the regulation imposes severe fines for violating its standards, with penalties potentially reaching tens of millions of euros. The GDPR shows Europe's commitment to data privacy and security as more individuals share personal data with cloud services, amidst frequent data breaches. The regulation is extensive and lacks detailed guidelines, still making compliance challenging (Wolford, 2018). As the internet is more integrated into daily life, it is essential for individuals to have the same rights online as they do offline. Human rights principles like freedom of expression, privacy, and societal participation are important in the digital world. Strong cybersecurity policies are needed to protect digital privacy and maintain these rights. Without trust in data security, people may self-censor and withdraw from online activities, harming fundamental rights. The Digital Services Act (DSA) and the Digital Market Act (DMA) are rules for the entire EU. Their two main goals are to ensure a safe digital environment that protects users' rights and to create fair competition that encourages innovation, growth, and global competitiveness. The Digital Services Act (DSA) mainly addresses online intermediaries and platforms like marketplaces, social networks, and app stores. Very large platforms and search engines with over 45 million monthly users in the EU have the strictest rules. The Digital Markets Act outlines rules for gatekeeper platforms that connect businesses and consumers, which also overlap with some DSA regulations but serve different purposes (European Commission, 2022). There are still important gaps and legal challenges to tackle, as some big platforms have significant control over important parts of the digital economy. They act as gatekeepers in digital markets and can create their own rules, which can lead to unfair situations for businesses that use these platforms and limit choices for consumers.

Western Balkans Cases of Cyber Safety

Albania has several key laws that affect cybersecurity. Law No. 9880/2008 on Electronic Signature outlines the rules for using electronic signatures. Law No. 107/2015 on Electronic Identification and Trust Services details the guidelines for safe electronic identification, seals, transmission services, and website authentication. Law No. 10128/2009 on Electronic Commerce sets rules for e-commerce, consumer privacy, and penalties for violations, also applying to online media with subscription services for revenue. The Assembly of Kosovo passed two laws related to cybersecurity in 2012. The Law on Information Society Services, adopted on 15 March 2012, covers electronic services such as e-commerce, e-payment, e-banking, e-government, and e-procurement. It aims to prevent issues and abuses in electronic transactions while securing information systems. The Law on Electronic Communications, adopted on 4 October 2012, sets legal standards for electronic communications and protects personal data and privacy rights. Whereas the Ministry of Public Administration, Digital Society and Media in Montenegro handles the legal framework and cybersecurity policy, such as the Electronic Commerce Act that supports the modern approach to cybersecurity in the country (Electronic Commerce Law, n.d.). In Serbia, civil society representatives and the Cybersecurity Network Foundation highlight that digitalization and ICT security are not being integrated, with (cyber)security and human rights not viewed as important parts of the digital process. Conversely, the Ministry of Trade, Tourism and Telecommunications sees a connection between information security, digitalization, and e-commerce. Their approach involves sharing data protection responsibilities with citizens by improving their digital skills, allowing them to protect themselves and exercise their rights fully.

The Law on Personal Data Protection in North Macedonia was first created in 2005 to introduce the right to privacy and protect citizens' personal data. A new version of this law was adopted in February 2020 to align with the EU's General Data Protection Regulation (GDPR). Legal entities were given 18 months to adapt to the new law, which fully took effect on 24 August 2021.

Bosnia and Herzegovina aims to enhance the security of its digital networks and information systems as part of its EU accession efforts. It plans to change its national laws to comply with the 2008 Stabilization and Association Agreement with the European Commission, which includes following the Council of Europe Convention on Cybercrime and the EU's General Data Protection Regulation.

Digitalization and EU integration are key factors driving cybersecurity policymaking, but this presents challenges. The six economies involved need to work on their commitments to human rights in their cybersecurity policies, focusing mainly on protecting networks and systems. This leads to cybersecurity resources being directed mainly at technical systems rather than user rights, which means that today time and investments have to be made for a more human-centric approach to cybersecurity (Klopfer et al., n.d.).

User Knowledge and Awareness and Best Practices for Safeguarding Personal Information

Users' low awareness increases their risk of identity theft, scams, and manipulation. A major barrier to better online data privacy is low digital literacy. Many users do not know about privacy settings, the meaning of terms of service, or the importance of secure communication tools. Closing this gap is key to helping users manage their online privacy effectively. User can ask for their personal data to be erased if it is not needed or is being misused; this is called "the right to be forgotten". For example, users should be aware that they can ask a company for access to their personal data, and have the right to receive a copy for free in a usable format. General Data Protection Regulation obligates that the company must respond within one month and provide data along with details on its use. When a company wants user's consent, they must clearly agree, such as by signing a form or choosing 'yes' on a webpage. Just opting out is not enough; user must actively agree to your data being stored or reused. Before user agrees, they should receive details about the company processing your data, why they use it, how long, who else received it, the user's rights, the company's contact info, and the Data Protection Officer's contact if applicable. The user can withdraw their consent for a company or organization by contacting the data controller. If an organization data based on their legitimate interest or public tasks, user might have the right to object, but in some cases, their public interest might allow them to continue using user's data, such as for scientific research. For direct marketing emails, a company needs user's consent to send them. For a current customer, they can send emails about similar products, users can object to these marketing emails at any time, and they must stop using user's data right away. Companies must inform user of their right to object during their first contact with user. If a company has shared user's data online and user request its deletion, the company must inform other sites where the data was shared. However, some data may not be deleted due to the need to protect rights

like freedom of expression, especially if it serves public interest. When it comes to children's rights, children usually need a guardian's approval to use online services that require personal data, like social media or downloading music and games. They won't need consent anymore once they are over 16 years old, or as low as 13 in some EU countries. Parental consent checks must be effective, such as through verification emails (European Union, 2019). Low digital literacy significantly increases users' vulnerability to identity theft, scams, and manipulation, as many individuals lack awareness of privacy settings, secure communication tools, and their rights regarding personal data protection. Under the General Data Protection Regulation, users are granted crucial rights such as access to their personal data, the right to be forgotten, informed consent, the ability to object to their data processing, and additional protections for children. This aims to strengthen individual control over personal information online.

Conclusion

Digital platforms offer convenience but collect personal data, including basic details and sensitive information about users' behavior, online activity footprints, and health information. This data is often shared with third parties, like advertisers, without users' clear consent, and it can be exploited for profit. This emphasizes the need for strong cybersecurity measures as part of human rights, as human rights cover both physical and digital spaces, where personal information is often collected and shared. Threats like surveillance and cybercrimes endanger individuals' freedoms, making it crucial to protect privacy to allow safe navigation of the digital world. Digital platforms must be clear about how they collect data and get users' consent before using their information. Strong security measures are also needed to prevent unauthorized access and data breaches. Platforms may not always meet these standards, so governments and international organizations need to ensure they are held accountable and enforce better regulations. Laws like the General Data Protection Regulation in Europe help protect privacy and give individuals control over their data. Global cooperation is essential to tackle challenges related to international data processing.

Future research could explore the creation of stronger international agreements that ensure a consistent level of data protection across borders, making it more difficult for malicious actors to exploit differences in national laws. Action should focus on improving cybersecurity laws to protect individual rights. Some countries

have advanced data protection regulations, like the GDPR, but many regions still lack strong privacy laws. Governments need to research and develop legal frameworks to tackle new cybersecurity threats, including surveillance and complex cyberattacks, while safeguarding sensitive personal data. Additionally, there is a need to investigate the ethical implications of cybersecurity technologies and their potential to infringe upon individual freedoms. Legal systems should integrate human rights principles into the development of cybersecurity laws, ensuring that the balance between security and privacy is maintained. Equal importance holds the investing in public education about data privacy and digital security. Therefore, education campaigns for vulnerable groups can help them manage their digital identities, the dangers of sharing personal information online, and the effects of data breaches. Research can explore the effectiveness of privacy tools like end-to-end encryption and how to make them accessible, helping people to protect their data and improve digital security.

Digital literacy programs should be included in school curricula globally to teach students about privacy, data protection, and cybersecurity, promoting a culture of responsibility and awareness in the digital world.

International understanding of regulations could encourage platforms to create systems that prioritize user consent, allowing people to easily opt in or out of data collection. This can reduce data misuse and protect digital rights.

Bibliography

Barykin, S.Y., Kapustina, I.V., Kirillova, T.V., Yadykin, V.K. and Konnikov, Y.A. (2020). Economics of Digital Ecosystems. Journal of Open Innovation: Technology, Market, and Complexity, 6(4), p.124. doi:https://doi.org/10.3390/joitmc6040124.

Electronic Commerce Law. (n.d.). Available at: https://ecommerce4all.me/wp-content/uploads/sites/6/2022/08/law-on-electronic-trade_en_zakon-o-elektronskoj-trgovini.pdf [Accessed 15 Jan. 2025].

European Commission (2022). The Digital Services Act package | Shaping Europe's digital future. digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

European Commission (2023). Data protection explained. [online] European Commission. Available at: https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

European Union (2019). Data protection. [online] Your Europe - Citizens. Available at: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_en.htm.

Klopfer, F., Bavcic, E. and Merali, L. eds., (n.d.). Cybersecurity and Human Rights in the Western Balkans: Mapping Governance and Actors.

Morić, Z., Dakic, V., Djekic, D. and Regvart, D. (2024). Protection of Personal Data in the Context of E-Commerce. Journal of Cybersecurity and Privacy, 4(3), pp.731–761. doi:https://doi.org/10.3390/jcp4030034.

ScienceDirect (n.d.). *Transactional Data – an overview* https://www.sciencedirect.com/topics/computer-science/transactional-data.

United Nations (1948). Universal Declaration of Human Rights. [online] United Nations. Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights.

Wolford, B. (2018). What is GDPR, the EU's new data protection law? [online] GDPR.eu. Available at: https://gdpr.eu/what-is-gdpr/.