*Vasić Milica**
https://orcid.org/0000-0002-5964-3524

UDK: 342.738(4672EU+73)
Review article
DOI: 10.5937/ptp2502143V
Received on: April 2, 2025
Approved for publication on:
May 18, 2025
Pages: 143–161

THE LEGAL-REGULATORY GAP IN DATA PROTECTION BETWEEN THE EUROPEAN UNION AND THE UNITED STATES OF AMERICA – CHALLENGES AND IMPLICATIONS

ABSTRACT: In the era of global digitalization, the legal regulation of data protection has become a key challenge for international law and business. While the European Union establishes robust privacy standards through the General Data Protection Regulation (GDPR), the United States applies a fragmented approach through various federal and state laws, creating legal challenges in transatlantic data protection regulation. This paper analyzes the legal consequences of the regulatory gap between the EU and the United States, particularly in light of the annulment of the Privacy Shield agreement. Through comparative legal analysis and case studies, the paper explores how differing legal frameworks impact the global digital economy, user privacy, and international corporations. Special attention is given to the extraterritorial reach of the GDPR, its influence on U.S. legislation, and potential legal mechanisms that could contribute to regulatory harmonization. The paper highlights the need for harmonizing international data protection standards that establish a balance between legal security, privacy protection and encouraging innovation in the digital ecosystem.

*LLM, PhD Candidate and Teaching Assistant, University Business Academy in Novi Sad, Faculty of Law for Commerce and Judiciary, Novi Sad, Serbia, e-mail: milica.vasic@pravni-fakultet.info

Keywords: *GDPR, CCPA, data protection, digital society.*

1. Introduction

Data protection has become one of the key global issues in the digital era. The advancement of technology and the omnipresent connectivity via the internet have enabled the seamless flow of data across borders, creating challenges in ensuring its protection. One of the most pronounced regulatory discrepancies arises between the European Union (EU) and the United States (U.S.). Although both sides recognize the importance of data protection, their legal approaches and regulatory frameworks differ significantly.

Data protection requires specific laws that are adapted to the specific circumstances in which data are used and the risks they may pose to individuals and to the democratic order. As new risks emerge, existing regulations need to be interpreted in the light of new knowledge and, if necessary, supplemented with new regulations. The European Union has followed precisely this principle (Schwartz, 2025, p. 112). The European Union has implemented strict regulations through the General Data Protection Regulation (GDPR). This sets high standards for data collection, processing, and protection. On the other hand, the United States has adopted a fragmented approach to data protection, relying on a combination of federal and state laws and industry standards. This legal discrepancy complicates the international data flow, causes disagreements between companies and legislators, and challenges internet users. Understanding these differences is crucial for developing international data protection agreements and achieving a balance between innovation, free data flow, and the right to privacy in today's digital society.

2. Methodological Approach

The research employs a multidisciplinary methodological approach that includes the analysis of legal documents, comparative legal analysis, and case study analysis. A qualitative analysis of legal documents, including the GDPR, CCPA, and relevant court decisions, has been conducted to identify key legal norms and their impact on the regulation of digital technologies. Comparative legal analysis provides insight into the regulatory differences between the EU and the U.S., aiming to identify similarities and differences in digital privacy regulation and the potential consequences of different approaches on global legal certainty and business operations. Case studies, focusing on companies such as Facebook and Ikea, offer insights into the

legal challenges of digital privacy and the global harmonization of legal regimes.

3. Research and Analysis

The development of digital technologies brings numerous benefits but also challenges in terms of their regulation at the global level. Countries adopt different approaches to regulating data protection and privacy, leading to legal inconsistencies and creating obstacles for international business (Mirković, 2023). The European Union (EU) has taken a proactive approach to data protection through the GDPR, which requires organizations to implement privacy safeguards in advance rather than merely responding after a data breach. The key principles of the GDPR include organizational accountability, maintaining records of data processing, conducting privacy impact assessments, and, when necessary, appointing a Data Protection Officer (General Data Protection Regulation (EU) 2016/679). Additionally, the GDPR mandates the implementation of privacy concepts by design and by default, ensuring data protection integration into technological systems from the outset.

A key dilemma in data protection is extraterritorial jurisdiction: States must protect their citizens beyond their borders, but over-application of the law can lead to legal uncertainty and make global business difficult (Czerniawski & Svantesson, 2023). In that sense, one of the GDPR's key characteristics is its extraterritorial scope, meaning that its rules apply even to companies outside the EU that process data of EU citizens (General Data Protection Regulation (EU) 2016/679). For example, American companies providing digital services to European users must comply with the GDPR, even if they do not have a physical presence in Europe. To avoid hefty fines, many U.S. companies, including tech giants like Facebook, have had to adjust their business practices to align with European privacy standards.

A culture of trust is the foundation of a secure digital environment in which individuals can be confident that their data is processed lawfully, ethically, and transparently. The GDPR contributes to building this culture through strict privacy protection standards and accountability requirements for organizations that collect and process data. However, a culture of trust is not built solely through legal enforcement but also through the adoption of responsible and ethical approaches to privacy protection. The GDPR establishes rules that help organizations earn and maintain users' trust, creating a safer digital environment where personal data is protected and privacy is respected.

However, the international data transfer between the EU and the U.S. remains legally problematic. This issue was initially addressed through the Safe Harbor agreement[1] in 2000, but it was invalidated by the EU Court of Justice in 2015 in the *Schrems I*[2] case due to inadequate data protection. Subsequently, in 2016, the EU and the US established the Privacy Shield as a replacement for Safe Harbour, which established that the US provided a "substantially equivalent" level of data protection to the EU. The mechanism entered into force on 1 August 2016 (Kuner, 2017.). Subsequently, the Privacy Shield agreement was established, which was also annulled in 2020 in the *Schrems II* case. In the Schrems II case (C-311/18), the European Court of Justice invalidated the Privacy Shield in 2020, concluding that U.S. laws still did not provide adequate EU citizens' data protection. Although the agreement was an improved version of Safe Harbor, it failed to establish effective privacy protection mechanisms. At the same time, the Court upheld the use of Standard Contractual Clauses (SCCs) for data transfers but emphasized that companies must individually assess whether data can be safely transferred to the U.S., considering the level of protection available there (Data Protection Commissioner v Facebook Ireland Ltd. and Maximillian Schrems (Schrems II), 2020, C-311/18, ECLI:EU:C:2020:559).

One of the most significant factors contributing to the deep regulatory gap between the European Union and the United States in the area of data protection is the mass surveillance practices carried out by the US government. Concerns about these practices are not new, but they

[1] Safe Harbor was an agreement between the EU and the U.S., established in 2000 by a decision of the European Commission (2000/520/EC), to allow U.S. companies to self-certify compliance with EU privacy principles without requiring individual approval from regulatory authorities. It enabled U.S. companies to transfer and process the personal data of EU citizens under specific privacy protection conditions, such as transparency, limited data usage, and adequate security measures. However, it failed to provide effective data protection, which led the European Court of Justice to annul it in 2015 in the Schrems I case, stating that it did not offer sufficient guarantees against surveillance by U.S. intelligence agencies, leaving EU citizens' data exposed to mass collection without proper legal safeguards (Weiss & Archick, 2016).

[2] Schrems I (C-362/14) was a case initiated by Austrian privacy activist Maximilian Schrems, challenging the legality of transferring EU citizens' data to the U.S. via the Safe Harbor agreement. The European Court of Justice ruled that Safe Harbor did not provide adequate protection, due to the potential for surveillance by U.S. intelligence agencies and the lack of legal remedies for EU citizens. As a result of the ruling, Safe Harbor was invalidated, and in 2016, the Privacy Shield was introduced to provide a higher level of data protection in transatlantic transfers (Court of Justice of the European Union. , 2015., Maximillian Schrems v Data Protection Commissioner, C-362/14, ECLI:EU:C:2015:650, Downloaded 2025, January 07 from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CA0362#ntr1-C_2015398EN.01000501-E0001).

have intensified significantly following the revelations made public by whistleblower Edward Snowden[3] in 2013. He exposed extensive surveillance programs carried out by agencies such as the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ), including programs such as PRISM, XKeyscore, and Tempora. These programs allowed for the systematic collection and processing of vast amounts of communications data, often without adequate judicial oversight or notification to citizens, and often in direct collaboration with private technology companies.

The revelations caused by Snowden's disclosures have triggered a deep crisis of trust in transatlantic relations in the field of digital policy, especially in the area of the transfer of personal data. On this occasion, the European Union has re-examined whether the US legal framework ensures an "adequate" level of data protection by Article 45 of the General Data Protection Regulation (GDPR). It was precisely the existence of unlimited powers of the US intelligence services, combined with the lack of effective legal remedies for non-US persons, that was one of the key reasons why the Court of Justice of the European Union annulled the Safe Harbor and Privacy Shield mechanisms in the Schrems I and Schrems II judgments. In the Schrems II case, the Court specifically stated that the US legal system does not provide foreigners with a comparable level of protection to that within the EU, and that the legal protection mechanisms in the event of abuse by US services are neither sufficient nor efficient. This assessment primarily stems from an analysis of the surveillance programs based on the Foreign Intelligence Surveillance Act (FISA), in particular Section 702, which allows the collection of electronic communications of foreigners outside the territory of the US without a court order. Foreign Intelligence Surveillance Act – FISA) is a federal law of the United States of America that was adopted in 1978 to regulate the procedures of electronic surveillance and collection of intelligence data related to foreign powers and their agents. FISA was originally enacted to establish a legal framework and oversight mechanism

[3] Edward Snowden is a former employee of the US National Security Agency (NSA) who, in 2013, disclosed classified information about the scope and nature of mass surveillance programs carried out by US intelligence services, including programs such as PRISM and XKeyscore. His revelations were first published in media such as The Guardian and The Washington Post, and the leaked documents indicated that US agencies were systematically collecting data on the electronic communications of millions of people worldwide, including EU citizens. After that, Snowden fled the US and was granted asylum in Russia. His findings have significantly influenced the global debate on the right to privacy, surveillance, and transatlantic data protection. (Encyclopaedia Britannica. (n.d.))

for activities involving foreign intelligence targets while respecting the rights of U.S. citizens. The FISA Amendments Act of 2008 introduced Section 702, a significant expansion of the powers of US intelligence agencies. The passage of Section 702 enabled the collection of electronic communications of foreigners located outside US territory without an individual court order. It means that the data can be collected directly from the Internet service provider or through the global Internet infrastructure. Therefore, it is not necessary to show reasonable suspicion or seek approval for a specific person; rather, mass programs such as PRISM and UPSTREAM (disclosed by Edward Snowden in 2013) are sufficient (Federal Bureau of Investigation, (n.d.)).

Section 702 of the Foreign Intelligence Surveillance Act (FISA), enacted in the United States of America, represents one of the most controversial elements in the analysis of the adequacy of data protection in the context of transfers from the EU to the USA. This one provision was introduced through amendments under the FISA Amendments Act of 2008. year, enables American intelligence agencies, primarily the National Security Agency (NSA), to collect electronic communications of foreigners who are outside the territory of the USA, without having to obtain it individual court order. The practice is based on the fact that the US services may target "non-US persons" abroad for the collection of intelligence data of importance for national security. Although approval is formally requested by the secret FISA court (Foreign Intelligence Surveillance Court – FISC), that approval does not refer to specific individuals but rather to general program and procedural guidelines, which enable mass and non-discriminatory data collection. In practice, this means that communications, emails, calls, and other digital data that pass through U.S. infrastructure — even if only in transit — may be subject to processing.

The issue recognized by the Court of Justice of the European Union (CJEU) in the Schrems II judgment was the fact that individuals in the EU, whose data is being collected, do not have an effective legal remedy in the United States. Specifically, there is no mechanism through which an EU individual can find out whether their data has been subject to surveillance, nor any way to challenge such surveillance before an independent body.

Although, following Schrems II and negotiations between the European Commission and the U.S. government, U.S. President Joe Biden signed Executive Order 14086 on October 7, 2022, which provides for the establishment of the Data Protection Review Court (DPRC) as a key component in strengthening data protection in transatlantic relations — that

is, as the United States' response to the European Union's concerns regarding surveillance and legal protection of EU citizens. Under this executive order, the DPRC was established as an independent body that allows individuals from "qualifying countries" (including EU member states) to file complaints if they suspect they have been subjected to unlawful surveillance by U.S. intelligence agencies. The DPRC serves as the second, higher-instance body in a two-tier redress mechanism. Thus, the core concern lies not only in the scope and secrecy of surveillance programs but also in the asymmetry of rights: U.S. citizens enjoy certain constitutional protections regarding privacy, while foreigners abroad effectively do not have a comparable legal standing. This legal imbalance directly affects the assessment of adequacy under Article 45 of the GDPR, as the EU requires that individuals in third countries be provided with a level of protection that is "essentially equivalent" to that within the Union. In that context, Section 702 of the FISA remains one of the key arguments against the assumption that the United States provides adequate protection of the personal data of EU citizens, despite efforts to mitigate that impression through political and administrative measures (European Data Protection Board, 2023).

In this context, under the GDPR, the European Commission has the competence to issue adequacy decisions, i.e., to determine which third countries provide a comparable level of data protection. To date, the United States of America is not on that list, precisely because of structural differences in the legal systems, and in particular because of the broad powers of US intelligence agencies to monitor communications (European Commission, n.d.). As an interim solution, Standard Contractual Clauses (SCC) are applied in practice, but they require additional technical and organizational measures to mitigate the risks of inadequate data protection in third countries, which significantly increases the regulatory burden for companies. Unlike the EU, the U.S. does not have a unified federal data protection law. Instead, regulation is fragmented, with specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) for health data and the Children's Online Privacy Protection Act (COPPA) for children's privacy protection. However, no comprehensive national law regulates data protection as a whole.

The only significant law at the state level is the California Consumer Privacy Act (CCPA), which sets high data protection standards and gives consumers greater rights over their information (California Privacy Rights and Enforcement Act of 2020). In addition to California, it is important to

mention the states of Virginia[4], Colorado[5], i Connectitut[6] that have enacted their own data protection laws. However, in relation to CCPA, the laws of these states do not provide for the establishment of an independent body for the enforcement of the law, nor do they allow for private lawsuits, which indicates a somewhat weaker mechanism for the implementation and protection of consumer rights. Although the CCPA shares similarities with the GDPR, there are key differences between them. The GDPR requires an opt-in model, meaning users must actively consent to the processing of their data, while the CCPA uses an opt-out model, allowing users to subsequently prohibit the sale of their data. Additionally, the GDPR applies to all companies processing data of EU citizens, regardless of their location, while the CCPA applies only to companies operating in California. Due to legal fragmentation, companies in the U.S. must comply with different laws across various states, resulting in increased regulatory costs and legal uncertainty. The proposed federal law, the American Data Privacy Protection Act (ADPPA) aims to establish a unified legal framework for user privacy protection in the U.S. It was introduced in 2022 but has not yet been passed. The law would impose strict regulations on the collection, processing, and storage of personal data for U.S. residents, granting them rights to access, correct, and delete their data (Tolson, 2025, Still No Federal Data Privacy Law: What Happened to the ADPPA?, March 18). The ADPPA is designed to replace the fragmented state privacy laws with a single federal framework. Meanwhile, political disagreements, particularly regarding whether the law should supersede state regulations like California's CCPA, have prevented its enactment, at least for now. Tech giants like Facebook (U.S.) and IKEA (EU) must adapt their business models to comply

[4] The Virginia Consumer Data Protection Act (VCDPA), from January 1, 2023, grants Virginia residents the right to access, correct, delete, and have portability of their data, as well as the right to opt out of targeted advertising, data sales, and profiling. The law also requires data controllers and processors to implement appropriate security measures and adhere to the Data Protection Principles (PrivacyEngine. 2023).

[5] In addition to California, other U.S. states have adopted comprehensive data protection laws. The Colorado Privacy Act (CPA), which took effect on July 1, 2023, grants Colorado residents rights such as access, correction, deletion, and portability of their data. It also allows them to opt out of targeted advertising and data sales. The CPA requires data controllers to conduct data protection assessments for high-risk processing activities and to implement principles such as data minimization and purpose specification (Colorado Attorney General, n.d.).

[6] The Connecticut Data Privacy Act (CTDPA), from July 1, 2023, provides Connecticut residents with similar rights as the previous two laws, including the right to access, correct, delete, and portability of personal data, as well as the right to opt out of targeted advertising and data sales. The CTDPA also requires data controllers to honor global opt-out signals and implement appropriate data protection measures (Consumer Privacy Act, n.d).

with GDPR in the EU while simultaneously adhering to the more flexible regulations of the U.S.. This dual compliance creates additional regulatory costs and can affect the business strategies of international companies.

Facebook, as a global social network originating in the U.S., must align its operations with GDPR but has often faced scrutiny from regulators for mishandling user data (Houser & Voss, 2018, pp. 50–51). The Irish Data Protection Commission imposed fines on Facebook for privacy violations related to unclear user consent options. Facebook has implemented various changes to comply with GDPR, including obligations regarding data access, transfer, deletion, and improving data security. Although the platform has adopted most GDPR guidelines, there remain concerns about user data privacy. The European company and global retail giant, IKEA, is required to fully comply with GDPR as it operates in the EU and collects personal data from users. This includes enabling users to access, correct, delete, and transfer their data, as well as transparent consent mechanisms for cookies and personalized advertising. While IKEA is known for applying high data protection standards, it is essential for the company to continuously comply with all new rules and inform users of their rights, enabling them to control their data related to purchases, preferences, and other services. One example of GDPR implementation in practice is the mandatory user consent for using cookies on their websites and providing an opt-out option for personalized advertising. However, the IKEA France case highlighted challenges in employee privacy protection, as the company used surveillance without employee consent, resulting in regulatory sanctions. In 2021, a French court fined this company €1 million for illegally surveilling employees and job applicants. It was found that IKEA had used private detectives and accessed police databases to gather information about its workers, including details about their bank accounts and union activities (MyRhline, 2025, Espionnage chez IKEA France: un réseau d'espionnage de la direction démasqué, March 15). The IKEA case indicates serious challenges in GDPR implementation regarding employee privacy and employer accountability. GDPR requires employers to collect and process employee data solely in a lawful, transparent, and proportionate manner, which IKEA violated through systematic surveillance without informing or obtaining employee consent.

GDPR sets high data protection standards that affect the business models of both technology and retail giants. This underscores the importance of effective enforcement of data protection regulations and indicates the need for ongoing oversight of corporate practices in processing employee data to ensure effective privacy protection by European legislation. The cases of

Facebook and IKEA demonstrate that non-compliance with these rules can lead to significant penalties and undermine the trust of users and employees. In the modern digital environment, where data is considered one of the most valuable resources, the effective implementation of GDPR becomes a necessary element of sustainable business. Companies that timely and consistently align their practices with regulations eliminate legal risks and potential penalties and build long-term user trust, which is a key factor for competitiveness in the global market. GDPR, although challenging to implement, provides a framework that ensures responsible data management, achieving a balance between business interests and rights to privacy.

After the previous data transfer mechanisms, Safe Harbor and Privacy Shield were invalidated by the EU Court of Justice, the European Commission adopted a new EU-U.S. Data Protection Framework on July 10, 2023. This framework allows U.S. companies to legally receive data from the EU, provided they are certified by the U.S. Department of Commerce and adhere to enhanced privacy protection standards. Key innovations include restrictions on U.S. intelligence agencies' access to collected data, thereby reducing the risks of unauthorized surveillance, the establishment of a Data Protection Review Court, which provides EU citizens with a legal mechanism to protect their rights in cases of unlawful data processing, and stricter obligations for U.S. companies, which must now comply with more precisely defined standards regarding the processing and storage of European user data. Although the framework represents progress, legal uncertainty remains, as the EU Court of Justice could potentially invalidate this agreement in the future, similar to its actions with previous solutions (Batlle & van Waeyenberge, 2024).

4. Discussion: Challenges and Perspectives of Global Data Protection Regulation

Although the official rationale for the adoption of the GDPR was to harmonize the legislation of EU member states and strengthen individuals' control over their data, this regulation also aims to level the playing field for all technology companies (Houser & Voss, 2018). GDPR initially appears as a set of restrictive rules, but in reality, it provides a framework that enables companies to enhance their operations while simultaneously increasing user trust through privacy and data protection (Pit, 2024). By introducing high privacy standards, the GDPR not only protects consumers but also contributes to strengthening trust and the competitive advantage of European companies.

However, differences in the implementation of digital regulations across countries create legal uncertainty and hinder international transactions, particularly in areas of digital data management and privacy (European Company Lawyers Association, 2023).

National legislations still exhibit significant variations in the degree of implementation of digital regulations. This may undermine the effectiveness of international transactions and reduce legal certainty, especially in the fields of privacy protection and digital asset management, where legal frameworks and technologies often develop at different paces (Stojšić Dabetić & Mirković, 2024). Additionally, the lack of global harmonization allows companies to register their businesses in jurisdictions with more lenient laws to avoid strict regulations. This complicates law enforcement on an international level and highlights the need for regulatory alignment to ensure trust in the global digital economy. Through the GDPR, the European Union insists on preserving privacy as a fundamental human right and promotes digital solidarity through fair data use and the development of technologies that enhance privacy protection (European Data Protection Supervisor, 2020).

US companies such as Google and Facebook have gained a significant market advantage thanks to weaker privacy regulations in the US. The EU, through the extraterritorial application of the GDPR, is seeking to limit this advantage and enable fair competition for European technology companies. The fundamental differences in the regulations stem from different legal and philosophical approaches – in the EU, privacy is a fundamental right, while in the US, a commercial approach prevails. Edward Snowden's revelations about mass surveillance further influenced the collapse of the Safe Harbor mechanism and encouraged the EU to strengthen regulation and impose stricter standards on entities outside its territory. In this context, US companies must adapt their operations to European standards or risk losing access to the EU market.

The implementation of GDPR requires significant financial resources, both for technical and legal compliance. Companies like Meta (Facebook) have allocated billions of dollars to adapt their systems to comply with the new regulations. The European Data Protection Board (EDPB) imposed a record €1.2 billion fine on Meta (Facebook) for the illegal transfer of user data from the EU to the U.S. The decision was the result of an investigation by the Irish Data Protection Commission (IE DPA), which found that Meta had failed to align its practices with European regulations following the Schrems II ruling in 2020. Meta relied on Standard Contractual Clauses (SCCs) as the legal basis for data transfers, but European authorities determined that

this mechanism did not provide sufficient protection against U.S. intelligence agencies. The EDPB emphasized that the data transfers were systematic, repetitive, and continuous, exposing millions of European users to potential risks. In addition to the financial penalty, Meta was given a six-month deadline to cease illegal data transfers and align its operations with Chapter V of the GDPR, which governs international data transfers. This decision is part of a broader regulatory crackdown on tech companies operating in the EU, aimed at ensuring stronger user privacy protection and stricter GDPR enforcement. The case highlights the ongoing legal conflicts between the EU and the U.S. regarding data privacy. With the Privacy Shield agreement no longer in place, companies like Meta must find a new legal basis for processing and transferring data, further complicating global digital flows. GDPR mandates that data be encrypted and anonymized, increasing costs and technical challenges for companies processing user data from the EU. While GDPR aims to protect user data, its complexity can make it difficult for individuals to understand their rights, and excessive consent requirements lead to "privacy fatigue", where users ignore terms of service due to information overload.

Although GDPR has a broad extraterritorial reach, its implementation is challenging due to regulatory differences between the EU and the U.S. While the EU insists on strict privacy standards, the U.S. legal framework is more flexible, relying on market mechanisms and industry standards. This legal uncertainty complicates business operations for global companies, which must align their business models with different regulatory environments (Swensen, 2021). On one hand, GDPR imposes strict data protection mechanisms, while the U.S. legal framework allows greater flexibility in data usage, potentially giving some companies a competitive advantage.

In this context, it is important to highlight the differences between GDPR and CCPA – two regulations that share the goal of protecting user privacy but differ in their approach and scope. GDPR, as a European law, imposes strict requirements on companies worldwide that process EU citizens' data, whereas CCPA applies to companies operating in California that meet specific criteria. GDPR requires companies to implement privacy mechanisms in advance and proactively ensure compliance with user rights. GDPR mandates explicit user consent before data collection, while CCPA allows users to request access to their data and prohibits its sale retroactively but does not impose the same level of proactive measures as GDPR. Additionally, GDPR grants users a broader range of rights, including the right to correct and delete data, whereas CCPA primarily allows users to know what information companies collect

and with whom they share it. These legal differences create challenges for global companies that must comply with both regulatory frameworks.

Beyond the fundamental differences in data protection approaches, GDPR and CCPA also differ in enforcement and penalties for non-compliance. GDPR imposes stricter fines, up to €20 million or 4% of a company's global revenue, while CCPA prescribes lower monetary penalties but allows individuals to sue if their data is improperly processed. CCPA focuses more on consumer rights concerning data sales, whereas GDPR sets comprehensive privacy standards for all aspects of personal data processing. Furthermore, GDPR requires companies to clearly define the legal basis for data processing, while CCPA does not impose the same restrictions but gives consumers more control over their data use. GDPR applies to all organizations processing EU citizens' data, regardless of location, whereas CCPA has limited jurisdiction, applying only to certain companies. These differences impact global companies that must carefully balance the requirements of both regulatory frameworks to remain legally compliant.

One of the key questions in data protection is how to reconcile different legal approaches while enabling the seamless flow of data without compromising user privacy. The EU – U.S. Data Privacy Framework represents significant progress compared to previous cross-border data transfer mechanisms but still leaves many open questions. The European Commission aimed to address the key issues that led to the annulment of the Privacy Shield, particularly regarding U.S. intelligence agencies' surveillance and legal protections for EU citizens. On the other hand, legal uncertainty remains, as it is still unclear whether the Court of Justice of the European Union (CJEU) will deem the new framework fully compliant with GDPR privacy standards.

One of the key challenges is trust in the new legal redress mechanism. The Data Protection Review Court, established under this agreement, is supposed to provide legal remedies to EU citizens if their data is compromised in the U.S. However, it remains uncertain whether this court will be independent and effective in practice. If the Data Protection Review Court remains part of the U.S. executive system, its impartiality in cases involving U.S. security agencies' interests could be questioned.

Another important aspect is the long-term sustainability of the framework. Historically, the EU and the U.S. have already unsuccessfully attempted to resolve this issue twice – first with the Safe Harbor agreement and then with the Privacy Shield, both of which were invalidated by the CJEU. If the EU-U.S. Data Privacy Framework is challenged and annulled again, it would further increase regulatory and legal costs for companies.

From the perspective of global companies, the new framework provides temporary legal certainty, allowing them to continue transatlantic data transfers without fear of sanctions or administrative barriers. However, companies investing in long-term data protection strategies face a dilemma – whether to rely on this mechanism or take additional measures.

In the context of future digital privacy regulations, the question arises whether a bilateral agreement between the EU and the U.S. is sufficient or whether a global legal framework is needed. Organizations like the OECD and the United Nations could play a key role in developing international data protection standards, which would provide a more stable legal framework for the digital economy. The gap between GDPR and U.S. legislation will remain a central issue in global privacy regulation. While the EU insists on high data protection standards, the U.S. is gradually introducing partial reforms through laws like CCPA in California, which shows a tendency to align with European principles. However, despite the current EU-U.S. Data Privacy Framework, without a comprehensive legal framework, companies will continue to face regulatory uncertainties, while end users will experience varying levels of privacy protection depending on their location. The question remains – will the world move toward global harmonization of data protection, or will we continue to witness legal fragmentation that complicates international business and privacy protection?

5. Conclusion

In the digital age, data protection represents a key challenge for international law and the digital economy. Legal discrepancies between the European Union and the United States of America create legal challenges in the cross-border transfer of information. While the EU implements uniform and strict privacy standards through the General Data Protection Regulation (GDPR), the American approach is characterized by fragmented and sector-focused regulation at the federal and state levels. This mismatch makes international data exchange difficult and creates an atmosphere of legal uncertainty for organizations that operate globally. While GDPR ensures high privacy standards and extraterritorial application of its rules, the U.S. data protection system remains inconsistent, complicating the alignment of legal regimes.

Non–classical bilateral mechanisms, such as the Privacy Shield and the new EU-U.S. Data Privacy Framework, have proven to be temporary solutions that do not guarantee long-term stability in regulating cross-border data flows. These agreements often come under legal scrutiny and risk being annulled,

highlighting the need for a more sustainable global privacy framework. The lack of comprehensive international regulations complicates the operations of multinational companies and leaves users exposed to inconsistent data protection standards. While the EU-U.S. Data Privacy Framework represents an attempt to resolve a long-standing regulatory issue, the question remains about its legal sustainability. The dilemma is whether this framework works temporarily or can endure in the long run.

A comparison of GDPR and CCPA further highlights the regulatory differences between the EU and the U.S. Although both laws share the same goal – protecting user privacy – GDPR establishes comprehensive standards applicable to all organizations processing the data of EU citizens, whereas CCPA grants greater consumer rights but within the limited jurisdiction of California. The key difference lies in the legal approach: GDPR requires proactive compliance and the application of privacy-by-design principles, while CCPA allows users to prohibit the sale of their data but does not impose the same strict obligations on companies. These differences create complex regulatory challenges for businesses operating in both markets and underscore the need for further hybridization of legal standards.

GDPR has become a global model for data protection, whereas the U.S. continues to use a fragmented approach without a unified federal law. This regulatory disparity complicates transatlantic data transfers and creates challenges for businesses and legislators. While the EU–U.S. Data Privacy Framework represents an attempt to address these issues, a long-term solution could be federal data protection law in the U.S. that aligns with European privacy standards.

It is a fact that fundamental issues of systemic oversight and legal protection are not fully resolved. The European Union continues to express reservations about the U.S. data protection system precisely because of the persistent imbalance between national security interests and individual privacy rights, significantly affecting the further regulation of data transfers between the two sides of the Atlantic.

The future of digital data regulation will depend on the international community's ability to overcome legal differences and establish a stable, comprehensive legal framework that balances privacy protection, legal certainty, and technological development. The European Union will continue to enforce high data protection standards, while the United States is increasingly introducing partial reforms through laws such as CCPA, which align with European regulations. However, without clear and harmonized legal guidelines, global companies will continue to face regulatory uncertainties, while users will experience varying levels of privacy protection depending on their location.

The lack of consistent regulation and the complexity of regulatory requirements can be just as challenging as assembling IKEA furniture without instructions – all the components are there, but without a clear guide, there is a risk of misinterpretation and failed implementation. This is precisely why a panoptic solution and the harmonization of international regulations are necessary to ensure legal certainty, privacy protection, and the promotion of innovation in the digital economy.

Vasić Milica
Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu, Novi Sad, Srbija

PRAVNO-REGULATORNI JAZ U ZAŠTITI PODATAKA IZMEĐU EVROPSKE UNIJE I SJEDINJENIH AMERIČKIH DRŽAVA – IZAZOVI I IMPLIKACIJE

APSTRAKT: U eri globalne digitalizacije pravna regulativa zaštite podataka postala je ključni izazov međunarodnog prava i poslovanja. Dok Evropska unija postavlja robustne standarde privatnosti kroz Opštu uredbu o zaštiti podataka (GDPR), Sjedinjene Američke Države primenjuju fragmentirani pristup kroz različite savezne i državne zakone, što stvara pravne izazove u transatlantskoj regulativi zaštite podataka. Rad analizira pravne posledice regulatornog raskoraka između EU i SAD-a, posebno u svetlu ukidanja *Privacy Shield* sporazuma. Kroz uporednopravnu analizu i studije slučaja, autorka istražuje kako različiti pravni okviri utiču na globalnu digitalnu ekonomiju, privatnost korisnika i međunarodne kompanije. Posebna pažnja posvećena je ulozi eksteritorijalnog dometa GDPR-a, njegovom uticaju na američko zakonodavstvo i potencijalnim pravnim mehanizmima koji bi mogli doprineti harmonizaciji regulative. Rad ističe nužnost usklađivanja međunarodnih standarda zaštite podataka koji uspostavlja ravnotežu između pravne sigurnosti, zaštite privatnosti i podsticanja inovacija u digitalnom ekosistemu.

Ključne reči: *GDPR, CCPA, zaštita podataka, digitalno društvo.*

References

1. *Adequacy decisions,* European Commission, Downloaded 2025, January 13 from https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
2. Batlle, S. & van Waeyenberge, A. (2024). EU–US data privacy framework: A first legal assessment. *European Journal of Risk Regulation*, *15*(1), pp. 191–200
3. Colorado Attorney General. (n.d.). *Colorado Privacy Act (CPA)*. Downloaded 2025, March 19 from https://coag.gov/resources/colorado-privacy-act/
4. Consumer Privacy Act. (n.d.). *Connecticut Consumer Privacy Law (CTDPA)*. Downloaded 2025, March 19 from https://www.consumerprivacyact.com/connecticut-consumer-privacy-law/
5. Czerniawski, M., & Svantesson, D. (2024). Challenges to the extraterritorial enforcement of data privacy law–EU case study. Dataskyddet, 50, pp. 127-153. Downloaded 2025, March 19 from SSRN: https://ssrn.com/abstract=4698122
6. European Commission aiming to reform GDPR enforcement rules in cross-border cases, European Company Lawyers Association, February 2023, Downloaded 2025, January 14 from https://inhouse-legal.eu/digitalisation-gdpr/european-commission-aiming-to-reform-gdpr-enforcement-rules-in-cross-border-cases/
7. European Data Protection Board. (2023). *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*. Downloaded 2025, March 19 from https://www.edpb.europa.eu/system/files/2023-09/edpb_opinion52023_eu-us_dpf_hr.pdf
8. Federal Bureau of Investigation. (n.d.). *Foreign Intelligence Surveillance Act (FISA) and Section 702*. U.S. Department of Justice. Downloaded 2025, March 19 from https://www.fbi.gov/how-we-investigate/intelligence/foreign-intelligence-surveillance-act-fisa-and-section-702
9. Houser, K. A., & Voss, W. G. (2018). Gdpr: The end of google and facebook or a new paradigm in data privacy? *Richmond Journal of Law & Technology*, *25*(1), pp. 1–109 Downloaded 2025, March 19 from https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=1457&context=jolt
10. Kuner, C. (2017). Reality and illusion in EU data transfer regulation post Schrems. *German Law Journal*, *18*(4), pp. 881–918

11. Mirković, P. (2023). Digital assets – a legal approach to the regulation of the new property law institute. *Pravo – teorija i praksa*, *40*(suppl), pp. 17–31 https://doi.org/10.5937/ptp2300017M
12. MyRhline (2025). *Espionnage chez IKEA France: un réseau d'espionnage de la direction démasqué*. MyRhline. Downloaded 2025, January 10 from https://myrhline.com/type-article/espionnage-ikea-france/
13. Office of the Attorney General. (2020). *California Privacy Rights and Enforcement Act of 2020*. Downloaded 2025, January 08 from https://oag.ca.gov/system/files/initiatives/pdfs/20-0009A%20%28Privacy%29.pdf
14. Pit, R. (2023). Digitalization vs. GDPR—Friends or Foes?, *Copperberg*, Downloaded 2025, January 13 from https://www.copperberg.com/digitalization-vs-gdpr-friends-or-foes/
15. PrivacyEngine. (2023). *Virginia Consumer Data Protection Act (VCDPA): A comprehensive guide*. Downloaded 2025, March 19 from https://www.privacyengine.io/blog/virginia-consumer-data-protection-act/
16. 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, Downloaded 2025, January 16 from https://eur-lex.europa.eu/eli/reg/2016/679/oj
17. Schwartz, P. M. (2025). Spiros Simitis as Data Protection Pioneer, *G.W. J. Law & Tech. (JOLT)* pp. 102-118, https://dx.doi.org/10.2139/ssrn.5146813
18. Shaping a Safer Digital Future: a New Strategy for a New Decade, European Data Protection Supervisor, 2020, Downloaded 2025, January 14 from https://www.edps.europa.eu/press-publications/publications/strategy/shaping-safer-digital-future_en
19. Stojšić Dabetić, J., & Mirković, P. (2024). Digitalna imovina – novo poglavlje u regulisanju imovinskih prava [Digital property – a new chapter in the regulation of property rights]. In: Počuča, M. (ured.), *XXI međunarodni naučni skup „Pravnički dani – Prof. dr Slavko Carić" Odgovori pravne nauke na izazove savremenog društva* [*XXI International Scientific Conference "Legal days – Prof. Slavko Carić, PhD" The responses of legal sciences to the challenges of modern society*] (pp. 667–677). Novi Sad: Univerzitet Privredna akademija u Novom Sadu, Pravni fakultet za privredu i pravosuđe u Novom Sadu https://doi.org/10.5937/PDSC24667S

20. Swensen, D. (2021). Data Protection v. Facebook Ireland Limited and Maximilian Schrems: Where Do We Go from Here?. *Md. J. Int'l L.*, *36*(1), pp. 24–50
21. Encyclopaedia Britannica, *Edward Snowden*. Downloaded 2025, March 19 from https://www.britannica.com/biography/Edward-Snowden
22. Tolson, B., (2025). *Still no Federal Data Privacy Law: What happened to the ADPPA?* Downloaded 2025, January 14 from https://www-smarsh.com/blog/thought-leadership/no-federal-data-privacy-law-what-happened-ADPPA
23. Weiss, M. A., & Archick, K. (2016). US-EU data privacy: from safe harbor to privacy shield. *Report prepared for Members and Committees of Congress*, 19 March 2016, Downloaded 2025, January 15 from https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2016/cs2016_0076.pdf