Review article

CONSUMER PROTECTION AS A GEOPOLITICAL TOOL: THE EUROPEAN UNION'S POWER EXERCISED THROUGH LAW IN DIGITAL MARKETS

Dr. Andrea Labancz, PhD Student, Assistant Lecturer
University of Szeged, Faculty of Law and Political Sciences,
Institute of Business Law
Bocskai utca 10-12., 6721 Szeged, Hungary
labancz.a@gmail.com

ABSTRACT

The spread of disruptive technologies has fundamentally transformed B2C relationships, creating new opportunities as well as new forms of vulnerability. Digital platforms, algorithms and data-driven services have reshaped market dynamics and generated new power relations affecting states, businesses and individuals. In this context, the European Union occupies a distinctive position due to its economic weight and regulatory capacity, which increasingly exert global influence.

This study examines how the European Union indirectly shapes technological development and global business models through law, with consumer protection, particularly in digital and financial markets, serving as a key instrument of geopolitical significance. It argues that EU regulatory frameworks, including the GDPR, DSA, DMA, DORA, the AI Act and PSD3/PSR, not only structure the internal market but also compel global service providers to adapt, thereby producing effects beyond the Union's borders.

The analysis demonstrates that digital consumer protection extends beyond its classical function of individual rights protection. By addressing risks arising from algorithmic systems, data-driven influence and manipulative practices, it contributes to shaping market structures and establishing a distinctive European regulatory model. At the same time, in digital financial markets, consumer protection performs a stabilising function: by maintaining trust in financial systems, it supports the resilience and global position of the European Union.

Methodologically, the study is based on doctrinal legal analysis combined with an interdisciplinary approach. It examines key EU legal instruments in consumer protection, digital regulation and financial law, and evaluates their cross-border and international effects.

The paper concludes that the geopolitical significance of EU digital consumer protection lies not in its explicit objectives, but in its indirect effects: through ensuring a high level of consumer protection and internal market functioning, it contributes to shaping global market practices and strengthening the European Union's regulatory influence.

Keywords: *Consumer protection, Digital finance, Digital markets, Extraterritorial scope, Personal data*

1. INTRODUCTION

The intensive innovation processes characterising our era have fundamentally transformed the functioning of the economy. Within the European Union (hereinafter referred to as „EU"), a decisive turning point in the evolution of digital regulation was the adoption of the Digital Single Market Strategy in 2015.[1] From this period onwards, the EU gradually established a complex and multi-layered regulatory framework in order to address the challenges arising from digitalisation.

As digital markets evolved, it became increasingly evident that many of these challenges could no longer be reduced exclusively to traditional business-to-consumer (hereinafter referred to as "B2C") relationships and revealed that traditional consumer protection mechanisms may no longer, in themselves, provide adequate responses to the specific risks arising in digital markets. As a result, a new generation of digital regulation may be observed within the EU. A notable characteristic of this regulatory framework is that the legislator frequently associates consumer protection objectives with legal instruments that are not, in their primary nature, consumer protection measures. While classical consumer protection law focuses predominantly but not exclusively on consumer rights, unfair commercial practices or contractual imbalances arising in B2C relationships, the new generation of such consumer protection-oriented regulation centres on the governance of digital services.

In connection with the above, it should be emphasized that, the present paper does not seek to provide a comprehensive analysis of the consumer protection legal framework. Rather, its primary objective is to examine those legislative instruments adopted following the Digital Single Market Strategy that, although not formally belonging to the field of consumer protection law and primarily regulating other policy or regulatory areas, nevertheless explicitly identify consumer protection as one of their regulatory objectives.

In light of the above, the central research question of this paper is to what extent does the EU's digital consumer protection regulation contribute to shaping global market functioning and influencing the operation of economic actors outside the EU.

1 European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6 May 2015.

In order to answer this question, firstly, the paper identifies the legal instruments relevant from the perspective of the research and subsequently evaluates them on the basis of a uniform analytical framework. In each case, the analysis examines:

- the regulatory technique applied (directive or regulation);
- the consumer protection objective pursued by the legal instrument;
- the territorial scope of application;
- the personal scope of applications, specifically, the obligated market actors
- and the protected category of persons;
- as well as the international and geopolitical effects resulting from the regulation.

The research is based on doctrinal legal analysis, with particular regard to the interrelationship between consumer protection law, digital regulation and financial regulation. To determine which legislative acts should form the subject of the analysis, I searched the EU's official legal database, EUR-Lex, for regulations and directives adopted since 2015, using the keyword "consumer protection" in the full text of the acts. The search results obtained were then reviewed and narrowed down to those legislative acts that address issues related to digital markets.

2. CONSUMER PROTECTION LAW IN THE DIGITAL ECONOMY

Although the origins of consumer protection can be traced back to antiquity, its institutionalized form only emerged in the 20th century.[2] Despite its relatively late emergence, consumer protection has undergone rapid development, which resulted in a regulatory framework that incorporates both private-law and public-law mechanisms.

Private-law characteristics of consumer protection law governs legal relationships between natural persons and businesses with the contractual relationship constituting its central focus. It encompasses, *inter alia*, general terms and conditions and the prohibition of unfair contract terms, warranty and guarantee rules relating to defective performance, as well as breach of consumer contracts.[3] The enforce-

---

2 Van de Grift, L.; van Zon, K., *The European Parliament and the origins of consumer policy*, 2024, Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757647/EPRS_STU(2024)757647(-SUM01)_EN.pdf], Accessed 03 April 2026.

3 Fazekas, J.: *A fogyasztóvédelem magánjogi keretei – a fogyasztói szerződések sajátosságai*, in: Hámori, A, Hamar, F.; Neszmélyi, Gy.; Veres, Z. (eds.) Fogyasztóvédelem – Fogyasztóvédelmi jog, Budapest, 2025, pp. 164-189.

ment of these rules is typically initiated by natural persons themselves through judicial proceedings or alternative dispute resolution mechanisms. By contrast, public-law characteristics of consumer protection law relies on regulatory oversight and public enforcement mechanisms aimed at ensuring the proper functioning of markets and preventing practices that may harm natural persons as a group. Public-law characteristics of consumer protection law includes, among others, rules concerning unfair commercial practices, advertising, product safety, and market surveillance. Compliance with these requirements is monitored by designated public authorities, which may impose administrative sanctions in the event of infringements.[4]

Actors in the traditional consumer protection legal relationship are clearly identifiable actors, namely the consumer (natural person) and the trader (business). According to consumer protection laws, the trader is any natural or legal person who is acting for purposes relating to his trade, business, craft or profession and the consumer means any natural person who is acting for purposes which are outside his trade, business, craft or profession.[5]

Although numerous EU legal instruments exist in the field of traditional consumer protection, the Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market,[6] the Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights[7] and the Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts[8] are generally regarded as the core pillars of the EU consumer protection acquis.

---

4 Tóth, T.: Fogyasztóvédelmi közjog, 2022, Available at: [https://jak.ppke.hu/uploads/articles/12239/file/Fogyik%C3%B6zjogjegyzet%20-%20T%C3%B3th%20Tiham%C3%A9r.pdf], Accessed 30 May 2026.

5 It should be noted that certain traditional consumer protection rules contain slight variations in these definitions. The above concepts are based on the definitions provided by the traditional consumer protection framework.

6 Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council [2005] OJ L149/22 (Unfair Commercial Practices Directive).

7 Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council [2011] OJ L304/64 (Consumer Rights Directive).

8 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L95/29 (Unfair Contract Terms Directive).

Examining these legal instruments, it should be noted that they were predominantly adopted in the form of directives. While the Unfair Commercial Practices Directive and the Consumer Rights Directive are maximum harmonisation directives, the Unfair Contract Terms Directive is a minimum harmonisation directive. The primarily focus on the directives of B2C relationships and their aim is to ensure a high level of consumer protection. Accordingly, the parties defined in the cited directives are the consumer and the trader in the traditional sense. It is also a common characteristic in the directives that they do not contain an explicit extraterritorial dimension; consequently, their international and geopolitical effects remain largely indirect and stem primarily from the attractiveness and regulatory influence of the EU internal market.[9]

The emergence of digital markets has fundamentally transformed the environment in which traditional consumer protection rules operate. Recognising these challenges, the European Commission launched the Fitness Check on Consumer and Marketing Law[10] to assess whether the existing consumer protection acquis remained fit for purpose in the digital economy.[11] The evaluation found that, while the core principles of EU consumer protection law remained valid, parts of the framework required modernisation to address emerging digital market practices. These findings contributed to the New Deal for Consumers initiative,[12] which aimed to strengthen enforcement and adapt consumer protection rules to the digital environment.[13] One of the most significant legislative outcomes of this process was the adoption of the Omnibus Directive[14] as regards the better enforcement and modernisation of Union consumer protection rules.[15]

Since the adoption of these instruments, new forms of abuse have emerged in digital markets, posing significant risks to consumers, including algorithmic manip-

9 The above findings are based on the Art 1-3. of the cited legal instruments.

10 Commission Staff Working Document, Executive Summary of the Fitness Check of EU Consumer and Marketing Law, SWD(2017) 208 final, Brussels, 23 May 2017.

11 European Commission, Commission Staff Working Document – Executive Summary of the Fitness Check, SWD(2017) 208 final, Brussels, 23 May 2017.

12 European Commission, A New Deal for Consumers: Questions and Answers, MEMO/18/2821, 11 April 2018.

13 European Commission, A New Deal for Consumers: Questions and Answers, MEMO/18/2821, Brussels, 11 April 2018.

14 Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019 amending Council Directive 93/13/EEC and Directives 98/6/EC, 2005/29/EC and 2011/83/EU of the European Parliament and of the Council [2019] OJ L328/7 (Omnibus Directive).

15 Davida, Z., *Consumer Decision-Making Autonomy in the Digital Environment: Towards a New Understanding of National Courts' Obligation to Assess Ex Officio Violations of Fair Commercial Practices*, European Journal of Risk Regulation, Vol. 15, No. 4, 2024, pp. 1034-1037.

ulation, dark patterns and data-driven marketing.[16] Reflecting these challenges, the European Commission adopted the Digital Fairness Fitness Check,[17] which suggests that the consumer protection reforms may require further adaptation to emerging digital practices and environment.[18]

Nevertheless, the evolution of the digital economy has created new market phenomena and risks that traditional consumer protection instruments cannot always adequately address. Innovation-driven solutions, such as crypto-assets, decentralised systems, data-driven mechanisms, have become increasingly significant in digital markets. These solutions often operate outside the traditional consumer–trader relationship. Consequently, the EU has gradually developed a new generation of regulatory instruments which, while frequently pursuing consumer protection objectives, extend beyond traditional B2C relationships to cover innovation-driven market solutions.

3. THE GEOPOLITICAL DIMENSION OF EU REGULATION

The above mentioned approach enables EU rules to apply to businesses outside the EU and extends the EU's regulatory influence beyond its borders. Although this approach is most described, in formal terms, as a manifestation of extraterritorial legislation, critical perspectives argue that it should rather be understood as a market-based extension regulatory influence. This critical approach explains the phenomenon by the so-called Brussels Effect. According to the theory developed by Bradford, the effects of EU legislation frequently extend beyond the territorial borders of the EU, as multinational businesses adopt EU rules and apply them across their operations. This mechanism is based on the economic significance of the EU internal market, as access to that market often requires compliance with EU regulatory standards.[19] The Brussels effect manifests in two forms: *de iure* and *de facto*. The *de iure* effect occurs when third countries incorporate EU rules into their own legal systems. By contrast, the *de facto* effect refers to situations where market actors outside the EU comply with EU rules even in the absence of a legal

16 Castro, L., *User manipulation: thinking beyond dark patterns,* 2020, Available at: [https://uxdesign.cc/user-manipulation-thinking-beyond-dark-patterns-3d17cf408753] Accessed 03 April 2026.

17 Commission Staff Working Document, Fitness Check of EU Consumer Law on Digital Fairness, SWD(2024) 230 final, Brussels, 3 October 2024.

18 European Commission, Questions and Answers on the Digital Fairness Act, QANDA/24/4909, Brussels, 3 October 2024.

19 Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford university Press, New York, 2020, pp. 25-66.
Gstrein, O.; Zwitter, A., *Extraterritorial application of the GDPR: promoting European values or power?* Internet Policy Review, Vol. 10, No. 3, 2021, pp. 4-5.

obligation to do so. In such cases, businesses may find it more economically efficient to operate under a single set of standards across multiple jurisdictions than to adapt their activities to different regulatory regimes.[20] Similarly to Bradford, Gstrein and Zwitter interpret the expansive legislative activity as a power-based process. In their view, the spread of rules is driven not primarily by shared values, but by economic interests and constraints.[21] Considering the above, it may be evident that maintaining different operational standards across multiple jurisdictions would impose significant costs on multinational companies. From both an economic and an administrative perspective, it is often more efficient and predictable to apply EU regulatory standards across all markets in which they operate.[22]

The legal foundation of this regulatory approach can be found in the Treaty on the Functioning of the European Union.[23] Article 169 TFEU expressly requires the Union to ensure a high level of consumer protection and, through Article 169(2)(a)[24], links this objective to Article 114 TFEU, which provides the legal basis for internal market harmonisation measures.[25] Consumer protection is therefore not conceived as an isolated policy objective, but as an integral component of the functioning of the internal market, where goods, services, capital and persons circulate freely.[26] This relationship is further reinforced by Article 114(3) TFEU, which requires harmonisation measures to ensure a high level of consumer protection. Read together, a coherent legal framework must be established in which the internal market is created and maintained through harmonisation, while a high level of consumer protection remains a fundamental objective of that process.

The above developments may suggest that consumer protection in the digital environment extends beyond the protection of individual consumers. Although the primary objective of EU regulation remains the effective protection of consumers

20 Bernat, M.; Spera, F., *The De Jure "Brussels Effect": Current Legal Trends in the EU's Unilateral Regulatory Globalisation,* Studia Europejskie – Studies in European Affairs, Vol. 28, No. 4, 2024, p. 82.

21 Gstrein, O.; Zwitter, A., *op. cit.,* note 15, pp. 4-5.

22 European Commission, *"Once-Only" steers Europe towards simpler cross-border processes for a better Single Market, in line with the EU Competitiveness Compass,* 2025, Available at: [https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=881984524&navigatingVersions=true], Accessed 03 April 2026.

23 Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 [2016] OJ C202/1 (TFEU).

24 Article 169 TFEU (Lisbon).

25 Article 114 TFEU (Lisbon).

26 Article 26 TFEU (Lisbon).

and the proper functioning of the internal market, the cross-border spread of EU regulatory standards may generate significant geopolitical effects by influencing market behaviour and regulatory developments beyond the territorial borders of the Union. The following sections examine this phenomenon in greater detail.

4. ANALYSIS OF SELECTED LEGAL INSTRUMENTS

The growing scope of EU consumer protection regulation raises the question of whether consumer protection has evolved beyond its traditional function and has become a broader regulatory tool. To explore this issue, the following section analyses selected EU legislative instruments on the basis of the criteria outlined above, with particular attention to their potential geopolitical implications and extraterritorial effects.

These are:

- Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers[27]
- Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services[28]
- Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market [29]
- Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market[30]
- Proposal for Regulation of the European Parliament and of the Council on payment services in the internal market[31]

---

27 Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC [2023] OJ L 2023/2225 (Consumer Credit Directive 2).

28 Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 (Digital Content Directive).

29 Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35 (Payment Services Directive 2).

30 European Commission, *Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC* COM(2023) 366 final (Payment Sevices Directive 3).

31 European Commission, *Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010* COM(2023) 367 final (Payment Services Regulation).

- Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector[32]
- Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets[33]
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services[34]
- 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[35]
- 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[36]
- Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828[37]
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence[38]

---

32 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1 (Digital Resilience Act).

33 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40 (Markets in Crypto Assets Regulation).

34 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 [2022] OJ L277/1 (Digital Services Act).

35 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).

36 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 [2022] OJ L265/1 (Digital Markets Act).

37 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L 2023/2854 (Data Act).

38 The Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L 2024/1689 (AI Act).

4.1. Low Geopoliticial Effects

4.1.1. Consumer Credit Directive 2

The digitalisation of financial services has transformed consumer credit markets, creating new products and risks for consumers, such as buy-now-pay-later (BNPL) models. In response, the EU adopted Consumer Credit Directive 2, a predominantly maximum harmonisation instrument designed to ensure a high level of consumer protection in the digital credit market.[39] It should be noted that it may only have limited extraterritorial relevance, as it primarily governs credit relationships within the EU internal market.[40] Unlike general consumer protection legislation based on the consumer–trader relationship, the Consumer Credit Directive 2 reflects the specific characteristics of the financial sector by regulating the relationship between consumers and creditors or credit intermediaries, while imposing extensive information, conduct and creditworthiness assessment obligations on market actors.[41] By doing so, it uses the traditional consumer definition.[42]

Based on the above, it can be concluded that from a geopolitical perspective, the Consumer Credit Directive 2 has only limited significance. Nevertheless, it reflects the EU's ambition to establish high consumer protection standards in digital financial services, potentially increasing the international attractiveness of the European regulatory model.

4.1.2. Digital Content Directive

The rapid growth of the digital economy and cross-border e-commerce has created new opportunities, while also exposing legal fragmentation and uncertainty regarding digital content and digital services. At the same time, consumers have faced increasing difficulties related to the quality, accessibility and contractual protection of such services, undermining trust in the digital market.[43] To resolve this situation, the EU has adopted the Digital Content Directive that harmonises key aspects of contracts for the supply of digital content and digital services and aims to strengthen the digital single market while ensuring a high level of consumer protection.[44] Although it does not contain a general extraterritorial clause, it contributes to the development of a coherent regulatory framework for cross-border

39 Consumer Credit Directive 2 Preamble (1)-(13).

40 Consumer Credit Directive 2 Art. 2.

41 Consumer Credit Directive 2 Art. 3-5.

42 Consumer Credit Directive 2 Art. 3 (1).

43 Digital Content Directive Preamble (1)-(6).

44 Digital Content Directive Preamble (2).

digital services within the EU.[45] The Digital Content Directive enhances legal certainty and establishes uniform consumer rights regarding conformity requirements, updates, remedies and contract modifications. The instrument regulates traditional consumer–trader relationships and applies not only where consumers pay a price, but also where they provide personal data as consideration. By doing so, it uses the traditional definitions of consumer and trader.[46]

In light of the above, the conclusion may be drawn that, the Digital Content Directive has only limited significance from a geopolitical perspective, as its primary objective is the functioning of the digital single market. However, the establishment of uniform contractual standards for digital services may indirectly influence non-EU providers seeking access to the European market.[47]

4.2. Medium Geopolitical Effect

4.2.1. Payment Services Directive 2, and the Proposed Payment Services Directive 3 and Payment Services Regulation

The rapid digitalisation of payment services has led to the emergence of innovative payment solutions that were not adequately covered by the existing regulatory framework. At the same time, technological developments have increased market fragmentation, legal uncertainty and security risks, highlighting the need for harmonised rules and stronger consumer protection in the digital payments sector.[48] To solve such issues, the EU has established the Payment Services Directive 2 in a form of a maximum harmonisation directive, leaving Member States only limited discretion in the transposition of its provisions into national law.[49] Although the regulatory framework primarily governs payment services and the functioning of the payment market, consumer protection remains one of its explicit objectives. As stated in the preamble, the rules aim to ensure a high level of consumer protection in the use of payment services throughout the EU.[50]

From a territorial scope perspective, Payment Services Directive 2 applies to payment services provided within the EU, particularly where the payment service

45 Digital Content Directive Art 1-4.

46 Digital Content Directive Art 2 (5)-(6).

47 Wiśniewska, K.; Pałka, P., *The impact of the Digital Content Directive on online platforms' Terms of Service*, Yearbook of European Law, Vol. 42, 2023, pp. 388–406.

48 Payment Services Directive Preamble (1)-(7).

49 European Banking Federation, *PSD2 Guidance*, 2016, Available at: [https://www.ebf.eu/wp-content/uploads/2017/05/EBF_PSD2_guidance_September_2016.pdf] Acessed 31 May 2026.

50 Payment Services Directive 2 Preamble (4).

providers involved are located in the EU.[51] From a personal scope perspective it should be noted that, unlike traditional consumer protection instruments, it does not primarily regulate consumer–trader relationships but focuses on payment service providers.[52] Nevertheless, as these entities provide services on a professional and commercial basis, the relationship between payment service providers and payment service users retains several characteristics of traditional consumer protection law. The consumer protection dimension of Payment Services Directive 2 is reinforced by its express incorporation of the consumer concept. Article 4(20) defines a consumer as a natural person acting outside his or her trade, business or profession,[53] mirroring the traditional definition used in EU consumer law. Payment Services Directive 2 also requires the provision of clear, accessible and free information on consumer rights,[54] as well as substantive rights relating to payment accounts.[55]

The inclusion of both a consumer definition and consumer-specific safeguards demonstrates that consumer protection forms an integral part of the regulatory framework. Accordingly, Payment Services Directive 2 may be regarded as sector-specific legislation that combines market regulation with consumer protection objectives.

In light of the above, the conclusion may be drawn that Payment Services Directive 2 has only limited significance from a geopolitical perspective. Nevertheless, it reflects the EU's ambition to establish high standards of security, transparency and consumer protection in the digital payments sector, potentially increasing the international attractiveness of the European regulatory model.[56]

Since the adoption of Payment Services Directive 2, the retail payments market has undergone significant digital transformation. In order to establish a harmonised regulatory framework for digital payment services, the Commission prepared the Payment Sevices Directive 3 and the Payment Services Regulation. The Payment Sevices Directive 3 and the Payment Services Regulation modernise the EU framework for payment services and further harmonise the applicable rules across the EU. While Payment Sevices Directive 3 leaves limited discretion to Mem-

[51] Payment Services Directive 2 Art. 2-3.

[52] Payment Services Directive 2 Art. 1.

[53] Payment Services Directive 2 Art. 4 (20).

[54] Payment Services Directive 2 Art. 106.

[55] Payment Services Directive 2 Art. 85.

[56] Zetzsche, D.; Buckley, R.; Arner, D.; Barberis, J., *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, SSRN Electronic Journal, 2017, pp. 21-26, Available at: [https://www.researchgate.net/publication/317999278_From_FinTech_to_TechFin_The_Regulatory_Challenges_of_Data-Driven_Finance], Accessed 03 April 2026.

ber States, primarily in relation to authorisation and supervision, both instruments pursue the objective of ensuring a high level of consumer protection and supporting the functioning of the internal market.[57] The territorial scope of Payment Sevices Directive 3 and Payment Services Regulation would cover services provided within the EU,[58] and the personal scope would not rely on the traditional consumer–trader dichotomy, but primarily regulate payment and electronic money service providers.[59] Nevertheless, the concept of the consumer remains relevant, being defined as a natural person acting outside their trade, business or profession.[60] The proposed framework also introduces a range of user protection measures, particularly in relation to fraud prevention, transparency and access to redress mechanisms.[61]

The geopolitical impact of Payment Sevices Directive 3 and the Payment Services Regulation should be considered moderate. While their primary objective is the functioning of the internal market and the protection of payment service users, the establishment of uniform standards for a large integrated market may indirectly influence non-EU providers and encourage the adoption of similar regulatory approaches beyond the EU.[62]

4.3. High Geopolitical Effect

4.3.1. Digital Resilience Act

The Digital Resilience Act was adopted in response to the increasing digitalisation and interconnectedness of the financial sector, which have significantly amplified ICT-related risks and vulnerabilities.[63] Although the Digital Resilience Act is not primarily a consumer protection instrument, the objective of ensuring a high level of consumer protection is also reflected in its provisions.[64] Consumer protection is pursued indirectly through the enhancement of cybersecurity, operational resil-

---

57 Payment Sevices Directive 3 Preamble (37), (42), (73); Payment Services Regulation Preamble (40).

58 Payment Sevices Directive 3 Art. 2, Payment Services Regulation Art. 2.

59 These entities are subject to authorisation requirements, supervisory obligations, consumer information duties and operational resilience requirements.

60 Payment Sevices Directive 3 Art. 2 (21).

61 Payment Services Regulation Art. 50, Art. 81-85, Art. 56-60.

62 What PSD3 Could Mean for Your Payment Strategy (Even If You're Not in Europe), 2025, Available at: [https://www.linkedin.com/pulse/what-psd3-could-mean-your-payment-strategy-even-youre-europe-z022c], Accessed 03 April 2026.

63 Digital Resilience Act Preamble (1)-(2).

64 Digital Resilience Act Preamble (11).

ience and the reduction of ICT-related risks, thereby ensuring the reliable provision of financial services to consumers.

The territorial scope of Digital Resilience Act primarily covers financial entities and ICT third-party service providers supporting their activities operating within the EU.[65] It should be noted that the Digital Resilience Act does not contain a general extraterritorial clause. Nevertheless, its practical effects may extend beyond the EU, particularly where ICT service providers established in third countries provide services to financial entities operating in the EU.[66] From a personal scope perspective, Digital Resilience Act does not regulate the traditional consumer–trader relationship. Instead, it applies to a broad range of regulated financial entities, including credit institutions, payment institutions, electronic money institutions, investment firms, insurance undertakings, crypto-asset service providers and certain ICT third-party service providers.[67] The Digital Resilience Act does not identify consumers as a distinct protected category. Rather, it seeks to protect the stability and operational resilience of the financial ecosystem. Consumers may indirectly benefit from Digital Resilience Act, as secure and resilient financial services are essential for participation in the digital economy.[68]

From a geopolitical perspective, Digital Resilience Act has a significance that extends beyond the traditional objectives of financial regulation, given that it contributes to strengthening the EU's digital and financial resilience. Its geopolitical relevance is further reinforced by the fact that certain obligations may affect ICT third-party service providers established outside the EU. In particular, critical ICT third-party service providers established in third countries may continue to provide services to EU financial entities only if they establish a subsidiary within the EU.[69] This requirement may be viewed as reflecting the EU's broader objective of reducing strategic dependencies and enhancing regulatory oversight over critical digital infrastructure. Consequently, Digital Resilience Act may form part of the

65 Digital Resilience Act Art. 2.

66 According to Art 31 (12) of the DORA: „Financial entities shall only make use of the services of an ICT third-party service provider established in a third country and which has been designated as critical in accordance with paragraph 1, point (a), if the latter has established a subsidiary in the Union within the 12 months following the designation.".

67 Digital Resilience Act Art. 2.

68 European Insurance and Occupational Pensions Authority (EIOPA): *Digital Operational Resilience Act (DORA)*, Available at: [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en], Accessed 31 May 2026.

69 Digital Resilience Act Art. 31(12).

EU's wider geopolitical strategy aimed at increasing resilience and control in an increasingly digitalised and interconnected environment.[70]

4.3.3. Markets in Crypto Assets Regulation

The adoption of Markets in Crypto Assets Regulation was driven not only by the objective of protecting consumers and investors, but also by the EU's strategic interest in promoting innovation and the development of digital financial technologies. As recognised in the preamble of the Markets in Crypto Assets Regulation, EU financial services legislation should adapt to the requirements of the digital age and contribute to the development of a future-oriented and human-centred economy.[71] Markets in Crypto Assets Regulation therefore simultaneously pursues consumer-protection, innovation and competitiveness objectives.

The Markets in Crypto Assets Regulation establishes a uniform framework for the crypto-asset market. The aim of the Markets in Crypto Assets Regulation is the providing high-level of protection for consumers[72] and investors, the enhancement of transparency and the prevention of market abuse.

The Markets in Crypto Assets Regulation was adopted in the form of a regulation, ensuring the direct and uniform application of its provisions throughout the European Union. It establishes a harmonised regulatory framework for the issuance, offering and admission to trading of crypto-assets, as well as for the provision of crypto-asset services.

The territorial scope of Markets in Crypto Assets Regulation covers crypto-assets issued, offered to the public or admitted to trading within the EU, as well as crypto-asset services provided in the EU.[73] The applicability of the Markets in Crypto Assets Regulation depends not only on the place of establishment of the service provider, but also on whether crypto-assets or crypto-asset services are offered to participants in the EU market. Consequently, Markets in Crypto Assets Regulation may have practical effects on issuers and crypto-asset service providers established outside the EU where they seek access to the EU market or target EU

70 KPMG, *DORA – ICT Third-Party Service Providers*, 2024, Available at: [https://assets.kpmg.com/content/dam/kpmgsites/ie/pdf/insights/consulting/ie-dora-ict-third-party-service-providers.pdf], Accessed 31 May 2026.

71 Markets in Crypto Assets Regulation Preamble (1)-(9).

72 Markets in Crypto Assets Regulation Preamble (79), (80), (85), (89), (109).

73 Markets in Crypto Assets Regulation Art. 2.

investors. Accordingly, Markets in Crypto Assets Regulation may be regarded as having a limited but explicit extraterritorial effect.[74]

From a personal scope perspective, it should be noted that MiCA does not primarily regulate the traditional consumer–trader relationship. Instead, it focuses on the actors participating in the crypto-asset ecosystem and the provision of crypto-asset-related services.[75] The primary addressees of Markets in Crypto Assets Regulation are crypto-asset issuers and crypto-asset service providers, which are subject to authorisation, governance, disclosure and conduct-of-business obligations.[76] Unlike traditional consumer protection instruments, Markets in Crypto Assets Regulation does not contain a specific definition of the consumer. The protected category under Markets in Crypto Assets Regulation is therefore primarily retail crypto-asset holder rather than consumers in the traditional sense.[77] Nevertheless, retail holders occupy a functionally comparable position to consumers in traditional consumer protection law, as they are typically non-professional market participants exposed to significant informational asymmetries in their relationship with issuers and service providers.[78] In this respect, Markets in Crypto Assets Regulation extends the logic of consumer protection into the field of crypto-assets by granting retail investors safeguards similar to those traditionally afforded to consumers, particularly through extensive disclosure obligations, the requirement to provide a crypto-asset white paper, clear risk warnings and restrictions on misleading marketing communications.[79]

From a geopolitical perspective, Markets in Crypto Assets Regulation represents one of the first comprehensive regulatory frameworks for crypto-assets. Given the cross-border nature of crypto-asset markets, issuers and service providers seeking access to the EU market are required to comply with its rules, potentially contributing to the international diffusion of EU regulatory standards and strengthening the EU's influence in digital finance.[80]

---

74 Zetzsche, D. A.; Annunziata, F.; Arner, D. W.; Buckley, R. P., *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy,* European Banking Institute Working Paper Series No. 2020/77, 2020, pp. 10-18.

75 Markets in Crypto Assets Regulation Art. 2.

76 Markets in Crypto Assets Regulation Art. 4-6, 59-75.

77 Markets in Crypto Assets Regulation Art. 3. point 37: 'retail holder' means any natural person who is acting for purposes which are outside that person's trade, business, craft or profession;

78 Mantzouni, F., *Consumer Protection under MiCAR*, 2024, Available at: [https://pergamos.lib.uoa.gr/uoa/dl/object/3448071/file.pdf], Accessed 31 May 2026.

79 Markets in Crypto Assets Regulation Art. 5-9.

80 LLPO Law Firm, *The Impact of MiCA on Cross-Border Operations for Non-EU Crypto Businesses,* 2023, Available at:

4.3.4. Digital Services Act

The rapid expansion of online platforms has fundamentally transformed the digital economy. In response to the growing risks associated with the platform economy, the Digital Services Act establishes a comprehensive regulatory framework.

The Digital Services Act was adopted in the form of a regulation, ensuring the direct and uniform application of its provisions throughout the EU. The Digital Services Act recognises that responsible and diligent behaviour by providers of intermediary services is essential for the attainment of a high level of consumer protection.[81] It also exhibits an extraterritorial dimension, since it applies not only to intermediary service providers established within the EU, but also to intermediary services offered to recipients located in the EU, regardless of where the provider itself is established.[82]

It should be noted that the regulatory logic of the Digital Services Act differs from that of traditional consumer protection law. While conventional consumer protection rules are based on the bilateral relationship between the consumer and the trader, the Digital Services Act reflects the reality of digital markets, where access to goods, services and information is increasingly mediated by online platforms and other intermediary service providers.[83] Consequently, rather than regulating the consumer-trader relationship directly, the Digital Services Act primarily imposes obligations on the intermediaries that shape and influence that relationship. From a personal scope perspective, the Digital Services Act applies to a broad range of intermediary service providers. The obligated market actors include intermediary service providers, hosting service providers, online platforms and very large online platforms (VLOPs),[84] which exert a particularly substantial influence on the functioning of digital markets.[85] The Digital Services Act introduces, *inter alia*, a specific prohibition of manipulative interface design techniques (dark patterns),

[https://www.llpolawfirm.com/2023/11/17/the-impact-of-mica-on-cross-border-operations-for-non-eu-crypto-businesses/], Accessed 31 May 2026.

81 Digital Services Act, Preamble (3).

82 Moravcova, D., *Impact of the DSA Regulation on Very Large Online Platforms,* Central European Journal of Comparative Law, Vol. 4, No. 2, 2023, p. 166.; Rudohradská, S.: *Practical Application of the Digital Services Act – The Case of the Slovak Republic,* EU and Comparative Law Issues and Challenges Series (ECLIC*)*, Vol. 9, No. 1, 2025, pp. 521–540.

83 Digital Services Act Preamble (1)-(2).

84 European Commission, *Supervision of the designated very large online platforms and search engines under DSA*, 2026, Available at: [https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses], Accessed 03 April 2026.

85 Digital Services Act Preamble (76)-(79).

and transparency requirements for algorithmic systems.[86] The protected persons primarily consist of recipients of intermediary services, particularly consumers, defined in accordance with the traditional consumer law concept as natural persons acting outside their trade, business, craft or profession.[87] However, the Digital Services Act extends protection beyond consumers to all users participating in the digital economy through intermediary services.[88] Overall, the Digital Services Act establishes a sector-specific regulatory model in which consumer protection forms an integral part of platform regulation.[89]

From a geopolitical perspective, the Digital Services Act should be considered significant due to its extraterritorial scope. By applying to intermediary services offered to recipients located in the EU irrespective of the provider's place of establishment, the Digital Services Act may influence the practices of global platform operators seeking access to the EU market.[90]

4.4. Very High Geopolitical Effect

4.4.1. General Data Protection Regulation

Although the General Data Protection Regulation is closely connected to digital consumer protection and has significantly influenced the development of subsequent digital regulatory frameworks, it does not form the subject of detailed examination in the present research. One of the principal criteria for the selection of the analysed legal instruments was the explicit appearance of consumer protection, in particular the objective of ensuring a high level of consumer protection, within the regulatory framework. Unlike the legal instruments analysed in detail, the General Data Protection Regulation primarily pursues data protection objectives and does not expressly identify consumer protection as an autonomous regulatory goal. Nevertheless, its relevance cannot be overlooked, as it introduced several regulatory techniques that subsequently became characteristic features of new-generation digital regulation, including the use of a directly applicable regu-

86 Digital Services Act Art. 25, Art. 27.

87 Digital Services Act Art. 3(c).

88 Digital Services Act Preamble (2).

89 Mohanlal, C., *Investigation: Platforms still use manipulative design despite DSA rules*, 2025, Available at: [https://dsa-observatory.eu/2025/08/07/investigation-platforms-still-use-manipulative-design-despite-dsa-rules/#:~:text=This%20is%20prohibited%20by%20Article%2025%20of,design%2C%20structure%2C%20or%20functions%20of%20the%20platform], Accessed 3 April 2026.

90 Sonkova, M., *Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act,* pp. 15-21, Available at: [https://www.coleurope.eu/sites/default/files/research-paper/EDP_4_24%20Sonkova_0.pdf], Accessed 3 April 2026.

lation, the protection of natural persons as the central regulatory subject, and the application of an extended territorial scope capable of producing effects beyond the borders of the EU. For this reason, the General Data Protection Regulation is considered only to the extent necessary to illustrate the relationship between data protection and digital consumer protection, as well as the emergence of regulatory techniques later adopted by digital consumer protection legislation.

From a geopolitical perspective, the General Data Protection Regulation should be considered significant due to its extraterritorial reach and its influence on the data governance practices of organisations operating both within and outside the EU.[91]

4.4.2. Digital Markets Act

A significant new-generation legal instrument in the field of platform regulation is the Digital Markets Act, which sets out obligations for so-called gatekeeper platforms[92] with the aim of preventing distortions of competition and protecting users.[93] Although the Digital Markets Act does not identify the attainment of a high level of consumer protection as an autonomous regulatory objective, it expressly refers to the objective of ensuring a high level of data protection.[94] Given that the protection of personal data constitutes a traditional safeguard for natural persons and forms an increasingly important element of consumer protection in digital markets, the Digital Markets Act may also be examined from a digital consumer protection perspective. While the Digital Markets Act is primarily competition-law oriented, its provisions on data protection and its impact on market functioning and access to digital services affect consumers. Accordingly, consumer protection appears not as an autonomous regulatory objective but as a consequence of preserving contestable and fair digital markets.

The Digital Markets Act was adopted in the form of a regulation, ensuring the direct and uniform application of its provisions throughout the European Union. The territorial scope of the Digital Markets Act is broad, as it applies whenever core platform services are provided or offered to business users or end users in the EU, irrespective of the gatekeeper's place of establishment.[95]

91 Schwartz, P.M.: *Global Data Privacy: The EU Way*, New York University Law Review, Vol. 94, No. 4, 2019, pp. 771–818.

92 European Commission, *Gatekeepers Portal*, Available at: [https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en], Accessed 3 April 2026.

93 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 Markets Act) OJ L 265/1.

94 Digital Markets Act Preamble (64).

95 Digital Markets Act Art. 1 point 2.

From a personal scope perspective, unlike traditional consumer protection legislation, the Digital Markets Act does not focus on the bilateral relationship between consumers and traders. Instead, it regulates designated gatekeepers whose market position enables them to influence the conditions under which the protected persons, namely end users and business users access digital markets.[96] These platforms are subject to a range of obligations and prohibitions aimed at preventing unfair practices and preserving market contestability. The Digital Markets Act therefore protects a broader group of market participants than traditional consumer protection legislation. Furthermore, it does not employ the traditional concept of the consumer but instead uses the notion of the "end user", defined as any natural or legal person using core platform services other than as a business user.[97] This demonstrates that the Digital Markets Act departs from the classical consumer–trader framework and adopts a market-structure-oriented regulatory logic.

From a geopolitical perspective, the Digital Markets Act may be regarded as an example of the EU's use of regulation as a strategic instrument. By imposing obligations on gatekeeper platforms and applying to services offered to business users and end users in the EU irrespective of the provider's place of establishment, the Digital Markets Act may influence the conduct of globally operating digital platforms.[98] Furthermore, the broad territorial and personal scope of the Digital Markets Act may make territorial separation difficult in practice, thereby extending its practical effects beyond the EU. This is particularly relevant in the case of globally dominant platforms, such as Google, Apple, Meta, Amazon and Microsoft, whose operations are subject to the conditions laid down by the Digital Markets Act for access to the internal market.

4.4.3. Data Act

In recent years, digitalisation and the growing use of connected products have significantly increased the economic and social importance of data. As a result, data has become a key resource for consumers, businesses and public actors alike.[99] In order to meet the needs of the digital economy and remove obstacles to the functioning of the internal data market, the EU adopted the Data Act, which establishes a framework governing access to and use of data generated by connected

---

[96] Digital Markets Act Art. 2(16), Art. 2(20).

[97] Digital Markets Act, Art. 2(16) and (20).

[98] Nestoras, A., *The 'Brussels Effect' in Digitalisation and the Future of Transatlantic Relations,* European Liberal Forum, Policy Brief No. 4, Available at: [https://liberalforum.eu/wp-content/uploads/2022/01/Policy-Brief-4-The-Brussels-Effect-Digitalisation-and-the-Future-of-Transatlantic-Relations.pdf], Accessed 3 April 2026.

[99] Data Act Preamble (1).

products and related services.[100] The Data Act was adopted in the form of a regulation, ensuring the direct and uniform application of its provisions.

The territorial scope of the Data Act is broad and several of its provisions have practical effects beyond the EU. It applies to market actors whose products, services or activities concern the EU market, irrespective of their place of establishment.[101] The personal scope of the Data Act differs significantly from that of traditional consumer protection legislation, since it focuses not on the consumer–trader relationship but on the interactions among participants in the data economy. The obligated actors include, inter alia, manufacturers of connected products, providers of related services, data holders and providers of data processing services.[102] The protected category extends beyond consumers to all users of connected products and related services, including both consumers and business users. Although the Data Act places the concept of the "user" at the centre of its regulatory framework, it also contains a definition of the consumer. It defines a user as „a natural or legal person that owns a connected product or to whom temporary rights to use that connected product have been contractually transferred, or that receives related services,"[103] while a consumer is defined as a „natural person who is acting for purposes which are outside that person's trade, business, craft or profession."[104] Consequently, the concept of the user is broader than that of the consumer and encompasses both consumers and business users. Accordingly, the key protected actor is not exclusively the consumer as a contracting party, but the user as a data-generating actor whose access to, control over and ability to share data are to be ensured by the Data Act.

From a geopolitical perspective, the Data Act may be considered significant because several of its provisions apply irrespective of the place of establishment of the relevant market actor. As a result, it may affect the conduct of entities operating outside the EU where their products, services or data-related activities concern the EU market. The Data Act demonstrates how consumer protection in digital markets is increasingly pursued through data governance rather than solely through the regulation of individual consumer transactions.[105]

100 Data Act Preamble (4).

101 Data Act Art (1) point 3.

102 Data Act Art.

103 Data Act Art. 2(12).

104 Data Act Art. 2(23).

105 Schwartz, P.M.: *Global Data Privacy: The EU Way*, New York University Law Review, Vol. 94, No. 4, 2019, pp. 771–818.

4.4.4. AI Act

The AI Act was adopted in response to the growing use of artificial intelligence and the risks it may pose to individuals and society. As the first comprehensive horizontal framework for AI regulation, it seeks to promote trustworthy and human-centric AI while ensuring a high level of protection of health, safety and fundamental rights.[106]

Adopted as a regulation, the AI Act establishes harmonised rules for the development, placing on the market and use of AI systems throughout the EU. Unlike traditional consumer protection instruments, its primary objective is not consumer protection but the protection of fundamental rights and public interests.[107] Nevertheless, several of its provisions may be considered relevant from a consumer protection perspective, particularly those addressing manipulation, the exploitation of vulnerabilities, algorithmic bias and harmful automated decision-making.

The AI Act has a broad territorial scope. It applies not only to actors established within the EU but also to certain providers and deployers outside the EU where AI systems are placed on the EU market or their outputs are used within the EU.[108]

Its personal scope extends beyond the traditional consumer–trader relationship. The obligated actors include providers, deployers, importers, distributors and other actors involved in the development, placement on the market and use of AI systems.[109] Similarly, the protected category is broader than the consumer in the traditional sense, as the AI Act seeks to protect all natural persons whose health, safety or fundamental rights may be affected by AI systems.[110] Unlike traditional consumer protection instruments, the it does not employ the concept of the consumer as a central regulatory category.

From a geopolitical perspective, it should be noted that the AI Act has a high level of significance. It applies not only to providers established within the EU but also to certain actors operating outside the EU. As a result, the AI Act may influence the practices of global AI developers and providers seeking access to the EU market. In addition, by establishing the first comprehensive regulatory framework for artificial intelligence, the EU may position itself as a global standard-setter in

106 AI Act Preamble (1).

107 AI Act Preamble (1); Fossati, C.: *AI Systems and Product Liability in the EU: A Private International Law Analysis*, EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 9, No. 1, 2025, pp. 545–566.

108 AI Act Art. 2 point 1.

109 AI Act, Arts. 3(3), 3(4), 3(6), 3(7), 3(8).

110 AI Act Art. 1(1), Preamble (1) and (27).

this field.[111] The AI Act demonstrates how the protection of consumers and other affected persons is increasingly pursued through the regulation of digital technologies and AI systems rather than solely through traditional consumer–trader relationships.

5. EVALUATION AND SUMMARY

The analysis confirms that the geopolitical effects of EU digital consumer protection legislation are not uniform. Rather, the examined legal instruments may be categorized according to the intensity of their capacity to influence market actors beyond the borders of the EU.

The first category consists of provisions with limited geopolitical significance, such as the Consumer Credit Directive 2 and the Digital Content Directive. Although these measures contribute to the functioning of the internal market and may indirectly influence non-EU market actors seeking access to the EU market, their primary effects remain largely confined to contractual relationships within the EU.

The second category includes provisions with moderate geopolitical effects, namely Payment Services Directive 2 and the proposed Payment Services Directive 3 and Payment Services Regulation. These measures establish harmonised standards for digital payment services and consumer protection in a large integrated market, which may indirectly encourage the adoption of similar regulatory approaches by market actors operating outside the EU.

The third category comprises instruments with significant geopolitical effects, including Digital Resilience Act, Markets in Crypto Assets Regulation and the Digital Services Act. A common feature of these regulations is that they regulate sectors characterised by strong cross-border activity and impose obligations on actors whose services may be provided across national borders. As a result, they may influence the conduct of market participants operating outside the EU and contribute to the international relevance of EU regulatory standards.

The strongest geopolitical effects can be identified in the General Data Protection Regulation, the Digital Markets Act, the Data Act and the AI Act. These instruments combine broad territorial scope with regulatory models capable of influencing globally operating undertakings. Their practical significance extends beyond the EU because access to the internal market frequently requires compliance with the standards established by these regulations.

[111] Sonkova, *Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act*, pp. 21-26.

The examined legal instruments suggest that EU digital consumer protection regulation may contribute to shaping market behaviour beyond the borders of the Union. At the same time, the analysis suggests that the geopolitical effects of the examined legal instruments should not be understood as autonomous regulatory objectives. Rather, they appear to stem from factors such as the broad territorial scope of certain instruments, the economic significance of the internal market, and the pursuit of objectives including consumer protection, market integrity, data governance, operational resilience and the protection of fundamental rights. In this respect, the geopolitical dimension of digital consumer protection may be regarded as a consequence of the regulatory design of the examined instruments rather than an expressly declared policy objective.

REFERENCES

BOOKS AND ARTICLES

1. Bernat, M.; Spera, F., *The De Jure "Brussels Effect": Current Legal Trends in the EU's Unilateral Regulatory Globalisation,* Studia Europejskie – Studies in European Affairs*,* Vol. 28, No. 4, 2024
2. Bradford, A., *The Brussels Effect: How the European Union Rules the World*, Oxford university Press, New York, 2020, pp. 25-66
3. Davida, Z., *Consumer Decision-Making Autonomy in the Digital Environment: Towards a New Understanding of National Courts' Obligation to Assess Ex Officio Violations of Fair Commercial Practices*, European Journal of Risk Regulation, Vol. 15, No. 4, 2024, pp. 1034-1037
4. Fazekas, J.: *A fogyasztóvédelem magánjogi keretei – a fogyasztói szerződések sajátosságai*, in: Hámori, A, Hamar, F.; Neszmélyi, Gy.; Veres, Z. (eds.) Fogyasztóvédelem – Fogyasztóvédelmi jog, Budapest, 2025, pp. 164-189
5. Fossati, C.: *AI Systems and Product Liability in the EU: A Private International Law Analysis*, EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 9, No. 1, 2025, pp. 545–566
6. Gstrein, O.; Zwitter, A., *Extraterritorial application of the GDPR: promoting European values or power?* Internet Policy Review, Vol. 10, No. 3, 2021
7. Moravcova, D., *Impact of the DSA Regulation on Very Large Online Platforms,* Central European Journal of Comparative Law, Vol. 4, No. 2, 2023
8. Rudohradská, S.: *Practical Application of the Digital Services Act – The Case of the Slovak Republic,* EU and Comparative Law Issues and Challenges Series (ECLIC*)*, Vol. 9, No. 1, 2025, pp. 521–540
9. Schwartz, P.M.: *Global Data Privacy: The EU Way*, New York University Law Review, Vol. 94, No. 4, 2019, pp. 771–818
10. Wiśniewska, K.; Pałka, P.: *The impact of the Digital Content Directive on online platforms' Terms of Service*, Yearbook of European Law, Vol. 42, 2023, pp. 388–406
11. Zetzsche, D. A.; Annunziata, F.; Arner, D. W.; Buckley, R. P., *The Markets in Crypto-Assets Regulation (MICA) and the EU Digital Finance Strategy,* European Banking Institute Working Paper Series No. 2020/77, 2020, pp. 10-18

EU LAW

1. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007 [2016] OJ C202/1 (TFEU)
2. Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35 (Payment Services Directive 2)
3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation)
4. 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 [2022] OJ L265/1 (Digital Markets Act)
5. 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 [2022] OJ L277/1 (Digital Services Act)
6. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 [2022] OJ L333/1 (Digital Resilience Act)
7. Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 [2023] OJ L150/40 (Markets in Crypto Assets Regulation)
8. Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 [2023] OJ L 2023/2854 (Data Act)
9. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L 2024/1689 (AI Act)
10. Directive (EU) 2015/2366 of the European Parliament and the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35 (Payment Services Directive 2)
11. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1 (Digital Content Directive)

12. Directive (EU) 2023/2225 of the European Parliament and of the Council of 18 October 2023 on credit agreements for consumers and repealing Directive 2008/48/EC [2023] OJ L 2023/2225 (Consumer Credit Directive 2)
13. European Commission, *Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC* COM(2023) 366 final (Payment Services Directive 3)
14. European Commission, *Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010* COM(2023) 367 final (Payment Services Regulation)
15. European Commission, A Digital Single Market Strategy for Europe, COM(2015) 192 final, Brussels, 6 May 2015.
16. European Commission, Commission Staff Working Document, Executive Summary of the Fitness Check of EU Consumer and Marketing Law, SWD(2017) 208 final, Brussels, 23 May 2017
17. European Commission, Commission Staff Working Document, Fitness Check of EU Consumer Law on Digital Fairness, SWD(2024) 230 final, Brussels, 3 October 2024

WEBSITE REFERENCES

1. Castro, L., *User manipulation: thinking beyond dark patterns,* 2020, Available at: [https://uxdesign.cc/user-manipulation-thinking-beyond-dark-patterns-3d17cf408753], Accessed 03 April 2026
2. European Commission, *Gatekeepers Portal*, Available at: [https://digital-markets-act.ec.europa.eu/gatekeepers-portal_en], Accessed 03 April 2026
3. European Commission, *"Once-Only" steers Europe towards simpler cross-border processes for a better Single Market, in line with the EU Competitiveness Compass,* 2025, Available at: [https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=881984524&navigatingVersions=true], Accessed 03 April 2026
4. European Banking Federation, *PSD2 Guidance*, 2016, Available at: [https://www.ebf.eu/wp-content/uploads/2017/05/EBF_PSD2_guidance_September_2016.pdf], Accessed 31 May 2026
5. European Commission, *Supervision of the designated very large online platforms and search engines under DSA*, 2026, Available at: [https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses], Accessed 03 April 2026
6. European Commission, Questions and Answers on the Digital Fairness Act, QANDA/24/4909, Brussels, 3 October 2024
7. European Insurance and Occupational Pensions Authority (EIOPA): *Digital Operational Resilience Act (DORA)*, Available at: [https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en], Accessed 31 May 2026
8. KPMG, *DORA – ICT Third-Party Service Providers*, 2024, Available at:

[https://assets.kpmg.com/content/dam/kpmgsites/ie/pdf/insights/consulting/ie-dora-ict-third-party-service-providers.pdf], Accessed 31 May 2026

9. LLPO Law Firm, *The Impact of MiCA on Cross-Border Operations for Non-EU Crypto Businesses,* 2023 [https://www.llpolawfirm.com/2023/11/17/the-impact-of-mica-on-cross-border-operations-for-non-eu-crypto-businesses/] Accessed 31 May 2026
10. Mohanlal, C., *Investigation: Platforms still use manipulative design despite DSA rules*, 2025, [https://dsa-observatory.eu/2025/08/07/investigation-platforms-still-use-manipulative-design-despite-dsa-rules/#:~:text=This%20is%20prohibited%20by%20Article%2025%20of,design%2C%20structure%2C%20or%20functions%20of%20the%20platform] Accessed 03 April 2026
11. Nestoras, Antonios, *The 'Brussels Effect' in Digitalisation and the Future of Transatlantic Relations,* European Liberal Forum, Policy Brief No. 4 [https://liberalforum.eu/wp-content/uploads/2022/01/Policy-Brief-4-The-Brussels-Effect-Digitalisation-and-the-Future-of-Transatlantic-Relations.pdf] Accessed 03 April 2026
12. Sonkova, M., *Brussels Effect Reloaded? The European Union's Digital Services Act and the Artificial Intelligence Act,* pp. 15-21, Available at: [https://www.coleurope.eu/sites/default/files/research-paper/EDP_4_24%20Sonkova_0.pdf] Accessed 03 April 2026
13. Tóth, T.: Fogyasztóvédelmi közjog, 2022, Available at: [https://jak.ppke.hu/uploads/articles/12239/file/Fogyik%C3%B6zjogjegyzet%20-%20T%C3%B3th%20Tiham%C3%A9r.pdf], Accessed 30 May 2026
14. van de Grift, Liesbeth; van Zon, Koen, *The European Parliament and the origins of consumer policy*, 2024, Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757647/EPRS_STU(2024)757647(SUM01)_EN.pdf] Accessed 03 April 2026
15. What PSD3 Could Mean for Your Payment Strategy (Even If You're Not in Europe), 2025, Available at: [https://www.linkedin.com/pulse/what-psd3-could-mean-your-payment-strategy-even-youre-europe-z022c] Accessed 03 April 2026
16. Zetzsche, D.; Buckley, R.; Arner, D.; Barberis, J.: *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, SSRN Electronic Journal, 2017, pp. 21-26, Avaialble at: [https://www.researchgate.net/publication/317999278_From_FinTech_to_TechFin_The_Regulatory_Challenges_of_Data-Driven_Finance] Accessed 03 April 2026