INTERNATIONAL JOURNAL OF ACADEMIC RESEARCH IN ECONOMICS & MANAGEMENT SCIENCES

OPEN ACCESS JOURNAL

Vol 14, Issue 4, (2025) E-ISSN: 2226-3624

Strategic Approach to the Role of Normative Power and its Instruments in Eu Foreign Policy in the Digital Age: 2010–2025

Dr. Siddik Arslan

Deputy Secretary General of the Erzurum Metropolitan Municipality

Email: siddikarslan@hotmail.com

DOI Link: http://dx.doi.org/10.6007/IJAREMS/v14-i4/27019

Published Online: 29 November 2025

Abstract

The European Union is redefining its normative power identity in the digital age by integrating value-based foreign policy with strategic instruments. This article examines how the Union employs digital regulatory tools (General Data Protection Regulation, Digital Services Act, Digital Markets Act) and external norm diffusion mechanisms to generate normative effectiveness in foreign policy during the 2010–2025 period, analyzing under which conditions and through what processes this occurs. The theoretical framework combines normative power approach with social constructivism and strategic autonomy concepts to analyze the production, transmission, and internalization processes of digital norms. The research employs qualitative document analysis method, examining strategy documents, regulations, and international declarations published by the European Commission, European Parliament, and European Council through thematic content analysis. Findings demonstrate that the Union has influenced digital legislation in approximately one hundred and fifty countries by utilizing market leverage, discursive legitimacy construction, and co-design mechanisms. The General Data Protection Regulation has played a determining role in recoding global data protection standards, while the Digital Services Act and Digital Markets Act have established a global reference framework for platform regulation and competition policies. However, the Union's normative impact varies depending on conditions such as third actors' market dependency, intra-Union institutional coherence, and the intensity of global power competition. China's digital authoritarianism model and the United States' technological dominance strategy emerge as external factors constraining the Union's normative power capacity. The study reveals that normative power has transformed into forms of epistemic control and infrastructural hegemony in the digital age, and that the Union's effort to develop strategic instruments while preserving its value-based identity creates a structural tension between normative consistency and strategic flexibility. The article proposes developing indicators for measuring normative effectiveness, examining comparative normative competition dynamics, and empirically investigating norm internalization processes in third countries.

Keywords: Normative Power, Digital Sovereignty, European Union Foreign Policy, General Data Protection Regulation, Strategic Autonomy

Introduction

In the discipline of international relations, the concept of power has evolved into a multidimensional phenomenon shaped not only by military and economic capacity but also by the transmission of values, norms, and institutional frameworks. In the post-Cold War era, the European Union has emerged as an effective actor in the global order through the export of normative values, despite not being a military superpower in the classical sense. This effectiveness has been explained through the Normative Power Europe approach conceptualized by Manners (2002). According to Manners, the Union's foreign policy impact is related not to what it does, but to what it is—namely, the normative values that constitute its identity.

However, in the second decade of the twenty-first century, the structure of global power competition has been fundamentally transformed by new instruments such as digitalization, disinformation, platform capitalism, and data governance. The digital age has redefined the manner in which norms are produced, transmitted, and exported, creating new dynamics that both consolidate and challenge the effectiveness of the Union's normative power (Bradford, 2023; Benkler, Faris, and Roberts, 2018). In this context, the concept of digital normative power presents a critical area of examination both theoretically and practically for the 2010-2025 period.

The digital age has brought to the fore the concepts of epistemic warfare and information sovereignty. Control over data flows, algorithmic governance, disinformation, and platform regulation have created new foreign policy instruments that transcend classical diplomatic tools (Bigo, Isin, and Ruppert, 2019). These developments necessitate a redefinition of the Union's legitimacy as a global normative actor, its strategic effectiveness, and the scope of its instrument set. In particular, the General Data Protection Regulation, which entered into force in 2016, the Digital Services Act of 2022, and the Digital Markets Act stand out as concrete regulatory instruments of the Union's digital normative power.

The examined period of 2010-2025 constitutes a laboratory for this transformation from the Union's perspective. These years have been characterized by Middle Eastern policies following the Arab Spring, Russia's disinformation campaigns, the rise of China's digital authoritarianism model, and Europe's development of digital sovereignty discourse against American digital monopolies. In this context, the Union's normative power is being reconstructed not merely through value export but through strategic instruments such as digital infrastructure regulation, data protection standards, platform governance, and combating disinformation.

The concept of normative power rests on the assumption that the liberal norms inherent to the Union's identity can be universalized (Reinfeld, 2024; Egan et al., 2023; Pace, 2024: 868-881). However, the digital age has given rise to new forms of power that question the applicability and impact of normative power: digital authoritarianism, information manipulation, and platform geopolitics (Aral, 2020). This situation has compelled the Union both to strategically redefine its normative identity and to update its own instrument set. The

examined period has also been central to the Union's effort to balance its pursuit of strategic autonomy with its normative identity (Biscop, 2019). Particularly in the digital domain, an increasing tension is observed between the ethical, democratic, and human rights-oriented framework of normative power and strategic interests.

This article, proceeding from precisely this dual line of tension, analyzes how the Union has transformed its normative power in the digital age into strategic instruments, the role and effectiveness of these instruments in the foreign policy-making process. The fundamental objective of the article is to enable a rethinking of normative power theory in the age of digitalization and strategic competition and to empirically demonstrate how digital regulations function as foreign policy instruments. In the literature, it is observed that the Union's digital regulations are generally addressed from the perspective of internal market policy or technology law. However, the foreign policy dimension of these policies, particularly within the normative power framework, has not been sufficiently examined. This study fills this gap by revealing the strategic function of digital regulations within the Union's foreign policy instrument set and their normative effects in third countries.

In this context, the study seeks to answer the following fundamental research question: "During the 2010--2025 period, through which mechanisms and under which conditions does the European Union strategically exercise its normative power in foreign policy by using the regulatory instruments of the digital age (General Data Protection Regulation, Digital Services Act, Digital Markets Act, artificial intelligence ethical-compliance frameworks) and its external instruments (combating disinformation, cyber diplomacy, data adequacy decisions); and to what extent does this use increase policy adoption in third countries and indicators of legitimacy at the multilateral level?"

This problematique foregrounds three fundamental mechanisms: First is market leverage and the Brussels effect; the Union's regulatory capacity compels actors seeking access to global markets to comply with Union standards (Bradford, 2020). Second is discursive-legitimacy construction; consistent communication of the Union's digital rights and ethical framework creates a normative reference framework in multilateral arenas. Third is co-design and co-regulation; permanent institutionalization of normative values is ensured through data adequacy decisions, bilateral memoranda of understanding, and joint working groups.

The functioning of these mechanisms depends on three fundamental conditions: First is intra-Union institutional coherence and implementation capacity; the speed of secondary legislation, the effectiveness of oversight mechanisms, and the credibility of sanctions strengthen outward-oriented normative impact. Second is third actors' dependency on the Union market; high commercial dependency makes normative compliance costs acceptable and accelerates regulatory convergence. Third is United States-China competition intensity; the Union's normative impact strengthens in areas where competition is low or medium, while unilateral diffusion weakens in areas of high competition and multi-stakeholder standardization processes gain importance.

The hypothesis developed in response to this question is as follows: "The European Union's digital regulatory and diplomatic instruments increase the adoption of Union-compliant policies and regulations in third countries and strengthen multilateral legitimacy through

market leverage, discursive-legitimacy construction, and co-design mechanisms; this impact significantly strengthens when intra-Union institutional coherence and implementation capacity are high, the relevant actor's dependency on the Union market is substantial, and United States-China competition intensity is low or medium, and weakens under opposite conditions."

This hypothesis reinterprets normative power not as a fixed conceptual category but as a form of power with high strategic adaptation capacity that is empirically testable. For the hypothesis to be falsifiable, the study defines three fundamental dependent variables: First is regulation adoption and convergence; the conceptual and structural similarity of third countries' legislative texts to Union legislation, the generalization of Union standards in global platforms' default policies, and behavioral change following sanctions will be measured. Second is multilateral legitimacy indicators; references to Union terminology in multilateral documents, joint sponsorships, and civil society organizations' support for Union frameworks will be evaluated.

This perspective associates the Union's digital instruments not only with reflecting normative values but also with strategically increasing foreign policy effectiveness. The scope of the study is based on the period between 2010-2025 and examines three fundamental areas particularly among the Union's foreign policy instruments: digital regulation and platform governance (General Data Protection Regulation, Digital Services Act, Digital Markets Act), data governance and privacy standards (data adequacy decisions, cookie regulations), combating disinformation and information ecosystem management (codes of practice, cyber diplomacy toolbox). These three areas are the domains where the Union's normative power is strategically re-exercised in the digital age.

As a theoretical framework, the study addresses the concept of normative power together with the strategic power approach; it particularly blends the arguments of authors such as Manners (2002), Tocci (2007), Sjursen (2006), and Laïdi (2008) regarding normative power with discussions of strategic autonomy and digital sovereignty. This theoretical integration makes it possible to explain the Union's institutional transformation aimed at aligning its normative values with strategic interests. Particularly the post-2015 European Digital Strategy and digital sovereignty discourse concretize the transformation of normative values into strategic instruments. Additionally, Barnett and Duvall's power typologies enable the differentiation of the instrumental, structural, and discursive dimensions of normative power (Barnett and Duvall, 2005).

Empirically, the study is based on a qualitative research design. Documents from the Commission, Parliament, and External Action Service, policy strategies, regulatory texts, and strategic communication documents will be examined. Additionally, empirical evidence will be collected through similarity analyses between third countries' legislative texts and Union legislation, evaluation of global platforms' policy documents, and tracking of Union terminology in multilateral documents. This study discusses not only the transformation of the Union's normative identity in the digital age but also how this transformation affects normative competition at the global level. Particularly, comparison with China's Digital Silk Road initiative and American technology monopolies is important for positioning the Union's digital normative power.

Thus, the study proposes that normative power is no longer exercised solely through value transmission but through forms of epistemic and infrastructural control established over digital ecosystems. This situation suggests a new paradigm in which normative power is concretized through digital strategic instruments. The findings show that the Union's normative power has evolved both in content and form in the digital age, with a shift occurring from value export toward infrastructure-based normative hegemony. The expansion of Bradford's Brussels effect concept into the digital domain reveals the Union's regulatory capacity's impact on global standardization (Bradford, 2020, 2023). Thus, the Union has developed a new foreign policy model that articulates digital sovereignty and normative power.

The expected contributions of this study can be summarized as follows: First, by bringing together normative power theory with the geopolitical realities of the digital age, it underscores the new synthesis between values and strategy in the European Union's foreign policy. Second, by presenting empirical and falsifiable hypotheses on how digital regulations function as foreign policy instruments, it makes an original contribution to the international relations literature. Third, it demonstrates that the Union's regulations such as the General Data Protection Regulation, Digital Services Act, and Digital Markets Act are not merely technical legislation but strategic instruments of normative power. Fourth, by operationalizing mechanisms such as market leverage, discursive-legitimacy construction, and co-design, it explains through which mechanisms normative power operates. Fifth, it analyzes how conditions such as intra-Union institutional coherence, third actors' market dependency, and great power competition regulate normative impact. Sixth, it enables the empirical measurement of normative impact through observable indicators such as third countries' legislative texts, global platforms' policies, and multilateral documents. Seventh, by revealing that normative power in the digital age is exercised through forms of epistemic and infrastructural control, it conceptualizes new forms of power. Eighth, by offering a comparative perspective with the digital strategies of global actors such as China and the United States, it evaluates the Union's position in the context of global normative competition.

Literature Review

Research on the European Union's normative power identity and its foreign policy instruments in the digital age has undergone a marked conceptual and empirical transformation in the post-2010 period. This section examines national and international literature addressing the relationship between the EU's norm entrepreneurship, its quest for digital sovereignty, and its strategic autonomy efforts, within the framework of periodic transformations and concrete policy implementations.

The normative power concept articulated by Manners in 2002 defined the EU's capacity to shape the international order through values, norms, and rules rather than military capacity (Manners, 2002). This approach placed the diffusion of universal principles such as human rights, democracy, rule of law, and multilateralism at the core of EU foreign policy. However, the conceptualization of normative power has been subject to significant criticism in subsequent periods. Diez demonstrated that the EU's normative discourse shows inconsistencies in practice and is shaped by interest calculations (Diez, 2005). It has been

particularly noted that the EU compromises its value-based principles in areas such as energy security and migration management.

The impact of digitalization on international relations in the post-2010 period has opened a new research area in the normative power literature. Bradford's Brussels effect concept explains the EU's regulatory standards' norm-creating capacity in global markets (Bradford, 2020). Particularly with the entry into force of the General Data Protection Regulation in 2018, the EU has risen to the position of global norm entrepreneur in the field of digital rights (Yakovleva and Irion, 2020: 201-221). The Regulation has influenced international companies and third countries with its high standards regarding the protection, processing, and transfer of personal data. This regulation is evaluated as a concrete indicator of the expansion of the EU's normative power into the digital domain.

The concept of digital sovereignty has become central to the EU's quest for strategic autonomy in the post-2010 period. Pohle and Thiel have defined digital sovereignty as the capacity of states and regional organizations to make independent decisions regarding digital infrastructure, data management, and technology standards (Pohle and Thiel, 2020). The EU's efforts in this area particularly aim to reduce dependence on United States-based technology companies and counter China's state-supported technology diffusion. The European Data Strategy announced in 2020 set out the EU's data sovereignty objectives (Whyte, 2020: 196-210). This strategy envisages the creation of European data spaces, facilitation of data sharing, and imposition of strict rules on data transfers to third countries.

The adoption of the Digital Services Act and Digital Markets Act in 2022 has expanded the scope of the EU's digital regulatory power. The Digital Services Act imposes obligations on online platforms regarding content moderation, removal of illegal content, and user rights, while the Digital Markets Act aims to limit the market dominance of large technology companies (Keller, 2021). These regulations demonstrate that the EU combines its normative power with economic regulatory capacity. However, the challenges encountered in implementing these laws and the resistance of technology companies reveal the limits of the EU's regulatory power.

The concept of strategic autonomy has prominently emerged in EU foreign policy literature in the post-2010 period. Biscop has defined strategic autonomy as the EU's capacity to act independently in the fields of security, defense, and foreign policy (Biscop, 2019). This concept reflects the need for the EU to develop its own capabilities in the face of uncertainties in transatlantic security relations and China's rising power. Strategic autonomy in the digital domain includes dimensions of technological independence, cyber defense capacity, and protection of critical infrastructure.

The EU's norm entrepreneurship role in cybersecurity and cyber diplomacy has received increasing academic attention in recent years. Tikk and Kerttunen examined the EU's efforts to develop international norms in cyberspace and revealed both the inward-looking regulatory and outward-looking norm diffusion dimensions of the EU's cybersecurity strategy (Tikk and Kerttunen, 2018). The EU's Cybersecurity Strategy adopted in 2013 and its updated version in 2019 have set objectives for resilience against cyber threats, security of the digital single market, and global cyber stability (Karathanasis, 2025; Liebetrau, 2024: 705-720).

Artificial intelligence regulations constitute the most current dimension of the EU's normative agenda in the digital domain. The Artificial Intelligence Act proposed by the European Commission in 2021 envisages the classification of AI systems according to their risks and the imposition of strict rules on high-risk systems (Veale and Borgesius, 2021: 97-112). This regulation aims to set global norms regarding ethical use of AI, algorithmic transparency, and protection of fundamental rights. However, concerns that the EU's regulatory approach in this area may hinder innovation are discussed in the literature.

The EU's neighborhood policy and enlargement processes demonstrate concrete applications of normative power instruments. Lavenex and Schimmelfennig examined the role of the EU's conditionality mechanisms in transformation processes in Eastern Europe and the Western Balkans (Lavenex and Schimmelfennig, 2009: 791-809). However, the effectiveness of these mechanisms varies depending on the internal dynamics of target countries and the sustainability of the EU's attractiveness. The EU's cooperation programs with neighboring countries in the field of digital transformation include dimensions of technical assistance, capacity building, and standard harmonization.

The EU's normative role in global governance and multilateralism has gained new dimensions in the digital age. International cooperation and rule-making efforts on digital trade, data flows, and cybersecurity demonstrate the EU's agenda-setting capacity in multilateral platforms. However, the technological competition between the United States and China makes the EU's multilateral norm-creation efforts more challenging (Farrell and Newman, 2019).

The EU's digital public diplomacy and social media use are evaluated as new foreign policy instruments. Bjola and Holmes examined how digital diplomacy transforms traditional diplomatic practices and analyzed the communication strategies of EU institutions on digital platforms (Bjola and Holmes, 2015). The EU's efforts to create value-based narratives on digital platforms, engage with target audiences, and combat misinformation constitute new instruments of normative power.

The tension between normative power and realpolitik is concretely visible in the EU's digital policies. Hyde-Price demonstrated that the EU's value-based discourse conflicts with security and economic interests in practical applications (Hyde-Price, 2006). The EU's quest for balance between human rights concerns and economic interests in digital cooperation and technology trade with China exemplifies this tension.

The EU's norm diffusion efforts in digital literacy and digital participation are supported by programs targeting developing countries. The EU's digital transformation projects conducted within the framework of development cooperation include components of infrastructure investment, education programs, and regulatory capacity building (Bjola & Manor, 2024; Carmel, 2020; Karjalainen, 2023: 293-311). These programs provide concrete examples where normative values are supported by material instruments.

Data sovereignty and data localization policies constitute important dimensions of the EU's quest for digital sovereignty. Farrell and Newman examined the role of data flows in global economic and political relations and demonstrated how the EU's data protection regime

shapes global data governance (Farrell and Newman, 2019). The EU's granting of adequacy decisions in data transfer agreements with third countries functions as an instrument for exporting normative standards.

The security of digital infrastructure and protection of critical technologies are at the center of the EU's strategic autonomy agenda. The toolbox adopted by the EU in 2019 regarding fifth-generation mobile communication network security determined member states' common approach to infrastructure security (Barrett et al., 2024; Carrapico & Farrand, 2025: 1-10). This toolbox includes objectives of reducing dependence on high-risk suppliers and increasing supply chain diversity.

The EU's ethical approach in the field of artificial intelligence and autonomous systems foregrounds the concept of human-centric AI. The ethical principles developed by the European AI Alliance and the High-Level Expert Group envisage the development of AI in a manner respectful of human dignity, autonomy, and rights (Floridi et al., 2018: 689-706). This approach demonstrates the EU's effort to align technological progress with normative values. The use of digital tools during the pandemic demonstrated the EU's digital capacities in crisis management. The digital vaccine certificate application, cross-border data sharing, and coordination mechanisms revealed that the EU can effectively use digital tools in emergencies (Purnhagen et al., 2020: 297-306). However, establishing balance between privacy rights and public health during this process created normative dilemmas.

The relationship between climate change and digital transformation constitutes the EU's green digital transformation agenda. The carbon footprint of digital technologies, energy consumption, and sustainable digitalization strategies demonstrate the EU's efforts to integrate environmental norms with technological progress (Hilty and Bieser, 2017). The digital dimension of the European Green Deal reveals the intersection of these two agendas. While existing literature addresses the relationship between the EU's normative power, quest for digital sovereignty, and strategic autonomy efforts from different dimensions, studies examining these three conceptual areas in an integrated analytical framework remain limited. Particularly, how the EU's normative power instruments evolved with digital transformation, how the quest for strategic autonomy was reconciled with normative identity, and the systematic effects of these processes on the EU's global position during the 2010-2025 period have not been comprehensively researched. This research aims to fill the identified conceptual and empirical gap in an original framework combining normative power theory, social constructivism, and strategic autonomy concepts.

Theoretical Framework

Understanding how the European Union positions its normative power instruments in the digital age and the function of these instruments in its foreign policy strategy requires a multi-layered theoretical structure. This study employs the normative power approach as its foundation while using constructivism and digital diplomacy concepts as supporting frameworks, analyzing the European Union's digital normative power strategy through the data-concept-theory analysis triad.

Normative Power Approach and Its Digital Transformation

Manners (2002) conceptualized the European Union as an actor that creates influence through norms, values, and legitimacy, distinct from military and economic power. In this approach, power operates through persuasion and attraction rather than coercion; values such as democracy, human rights, and the rule of law are not merely discursive tools but structural components of the Union's identity (Manners, 2008). Normative power defines what the European Union is rather than what it does; this ontological characteristic constitutes the fundamental logic of the Union's foreign policy behavior (Reinfeld, 2024; Chaban & Elgström, 2024: 1-15). However, in the digital age, the instruments, scope, and legitimacy foundations of normative power have undergone transformation. While physical proximity, geographical neighborhood, and face-to-face diplomacy were prominent in the traditional understanding of normative power, digital technologies have enabled the instant, borderless, and mass-scale dissemination of normative content. This transformation has increased the Union's capacity to globalize its normative discourses while simultaneously bringing risks of distortion, manipulation, and confrontation with counter-narratives.

The functioning of normative power in the digital environment has different dynamics from traditional diplomatic channels. Social networks, digital platforms, and algorithmic content distribution have become new intermediaries determining which audiences, in which contexts, and how normative messages reach. The European Union's General Data Protection Regulation (GDPR) is a concrete example of this digital normative power. GDPR has become a binding norm not only within European borders but for all global actors engaged in commercial relations with the European Union. Bradford (2020) conceptualized this phenomenon as the "Brussels Effect" and demonstrated how the European Union's regulatory power shapes global market standards. The global acceptance of GDPR is the most evident proof that normative power is strengthened through digital instruments; however, this process also raises the question of whether the Union's normative claims constitute universal legitimacy or regulatory hegemony (Yilma, 2023; Eskhita & Stamhuis, 2024: 262-277).

Constructivism and Normative Identity Construction

Wendt (1999) argues that the meaning of anarchy in international relations is determined by the ideas and norms actors share. From this constructivist perspective, the European Union's digital policies are not merely technical regulations but material expressions of normative preferences regarding a particular world order. Finnemore and Sikkink (1998) define the life cycle of norms as a process that begins with "norm entrepreneurs," spreads through a "norm cascade," and becomes institutionalized through "norm internalization." The European Union assumes precisely such a norm entrepreneur role in the digital domain. The Digital Services Act and Digital Markets Act have established new norms regarding platform content responsibility, algorithmic transparency, and competition law; diplomatic, economic, and legal instruments have been used for these norms to gain global acceptance (Reinfeld & Gaon, 2025).

The constructivist approach shows that the European Union's digital normative power not only creates external influence but also reproduces the Union's own identity. The digital sovereignty discourse is the linguistic expression of the Union's search for technological independence, data autonomy, and a value-based digital order. This discourse reflects the

Union's search for a third way between China's state capitalism and the United States' market liberalism in the global digital economy (Laïdi, 2008). Digital sovereignty embodies the tension between the strategic instrumentalization of normative identity and the preservation of value integrity. While the Union seeks legitimacy through universal human rights discourse on one hand, it attempts to protect its economic and geopolitical interests through digital regulations on the other. This dual structure constitutes the inherent contradiction of normative power.

Digital Diplomacy and the Dissemination of Normative Discourse

Digital diplomacy refers to the transformation of traditional diplomatic practices through digital tools (Bjola and Holmes, 2015). This concept encompasses the ways states and international organizations share information, communicate, and create influence in digital environments. The European Union has positioned digital diplomacy as a strategic tool both in terms of content production and discourse dissemination. The European External Action Service and the Commission's digital units disseminate the Union's normative messages at the global level through social media campaigns, online events, and digital content strategies. Particularly during the 2022 Ukraine crisis, the Union conducted an active information and counter-narrative campaign on digital platforms; combating disinformation constituted a critical dimension of protecting normative discourse through digital tools (Mortensen & Pantti, 2023).

The most distinctive feature of digital diplomacy is its transition from unidirectional information flow to bidirectional interaction. Norms are no longer merely imposed top-down; they are discussed, interpreted, and reproduced on digital platforms. This dynamic process makes the European Union's normative power strategy more flexible and participatory while simultaneously making it more fragile and open to contestation. The constant conflict of normative discourse with counter-narratives and alternative value systems in digital environments reveals the limits of the Union's normative hegemony. For example, China's Digital Silk Road project and Russia's cybersecurity approach present alternative models to the European Union's digital normative discourse (Chander & Sun, 2023).

Data Analysis: Normative Discourse in Digital Policy Documents

Content analysis of the European Union's digital policy documents during the 2010-2025 period demonstrates that normative discourse is prominently featured. The European Commission's fundamental policy documents such as "A Digital Agenda for Europe" (2010), "Digital Single Market Strategy" (2015), and "Europe's Digital Decade" (2021) contain strong rhetoric aimed at protecting values and principles. In these documents, concepts such as personal data protection, digital privacy, algorithmic transparency, platform responsibility, and digital literacy are indicators of the Union's efforts to transfer its normative identity to the digital domain. However, the same documents also prominently feature interest-based emphases such as economic competition, strengthening European companies in digital markets, technological independence, and strategic autonomy. This dual discourse raises the discussion of the instrumentalization of normative power.

The European Union's 2013 and 2020 Cybersecurity Strategies in the field of cybersecurity demonstrate how normative values are integrated with security concerns (Maurer, 2021). These strategies emphasize that cyberspace should be open, free, and secure while also containing security-oriented objectives such as protecting critical infrastructures, deterring

cyberattacks, and resilience against digital threats. This intertwining of normative values with security priorities reveals that the European Union's digital normative power has a pragmatic character. Values also function as legitimizers of strategic interests rather than merely universal ideals.

Concept Analysis: Digital Sovereignty and Normative-Interest Synthesis

The concept of digital sovereignty is central to the European Union's normative power strategy. This concept has a multi-dimensional meaning encompassing technological independence, data autonomy, digital infrastructure control, and norm-setting power. While the digital sovereignty discourse expresses the Union's claim to determine the rules of the global digital order, it also reflects the search to escape technological dependence on the United States and China. This concept emerges as a domain where normative values are synthesized with strategic interests. For example, the European Union's Gaia-X project in cloud computing infrastructures carries both the objective of preserving data protection norms and increasing the competitive power of European companies in digital markets (Bradford, 2023).

The concept of digital sovereignty is also open to criticism regarding the instrumentalization of normative power. Some authors argue that the Union's digital regulations serve protectionist economic interests rather than universal values. Particularly the Digital Markets Act's targeting of large technology companies has provided grounds for these criticisms. However, the Union legitimizes these regulations with normative justifications such as protecting competitive markets and securing consumer rights. This situation shows that the discursive construction of normative power is intertwined with strategic calculations.

Theory Analysis: Critical Evaluation of the Normative Power Approach

Although the normative power approach provides a powerful framework for understanding the European Union's foreign policy, it contains certain theoretical limitations. First, measuring and verifying normative power is difficult. It is not always clear to distinguish which actions are performed with truly normative motivations and which with strategic calculations. Nye (2004) pointed to a similar ambiguity when developing the concept of soft power; isolating the causality of influence-creation processes is fraught with methodological difficulties. Second, the assumption that normative power operates on the basis of universal values may overlook cultural and regional differences. The fact that values such as digital privacy, freedom of expression, and algorithmic transparency advocated by the European Union are not perceived in the same way by every society, and can even be interpreted as Western-centric imposition in some societies, renders the universality claim of the normative power approach problematic (Keukeleire & Delreux, 2022).

Third, the relationship between normative power and material power is ambiguous. Keohane and Nye (2001) demonstrated with the concept of interdependence that states influence each other through norms and institutions; however, the role of material resources and economic asymmetry in this interaction cannot be ignored. The European Union's digital normative power is largely based on its economic weight, large internal market, and regulatory capacity. The Brussels Effect shows how the Union's market size strengthens its norm-dissemination capacity; this reveals that normative power is not merely about values but is based on material foundations (Bradford, 2020).

Information Asymmetry and Digital Inequalities

A critical theoretical issue brought by the digital age is information asymmetry and digital inequalities. While the European Union's normative messages can reach wide audiences on digital platforms, the ways these messages are received and interpreted differ depending on social, cultural, and economic factors. Factors such as digital literacy level, access to technology, digital infrastructure quality, and digital culture directly affect the effectiveness of normative power. For example, while the European Union's GDPR norms are more easily accepted in societies with developed digital infrastructure, their applicability remains limited in regions where digital divide is intense (Ragnedda & Gladkova, 2020). Therefore, the European Union's digital normative power strategy needs to be evaluated not only in terms of content production but also with dimensions of access, comprehensibility, and legitimacy.

Conclusion: Normative Power, Identity, and Legitimacy

The theoretical framework adopted in this study demonstrates that the European Union's use of digital normative power is not merely a foreign policy strategy but also a process of identity construction and legitimacy production. Normative values function as elements defining the Union's raison d'être and its position in the international system. Digital tools are strategic platforms used to make these values visible and disseminate them at the global level. However, the combination of these two elements, while enabling the European Union to develop a distinctive foreign policy model, creates a constant tension between normative consistency and strategic flexibility. The management of this tension is the fundamental determinant of the Union's sustainability as a normative power in the digital age.

Research Methodology

This research is based on a qualitative analysis (Braun & Clarke, 2022) examining how the European Union constructed digital norms at the global level during the 2010-2025 period and through which mechanisms these norms were integrated into foreign policy strategies. The fundamental problematic of the study is the process of redefining the EU's normative power identity through digital instruments. The research design aims to demonstrate that the EU's digital discourses do not remain merely at the rhetorical level but rather transform into concrete policy instruments and global normative structures, by placing the conceptual framework of social constructivism and critical norm theory on a methodological foundation. Positioned within the interpretivist paradigm, this study centers on actors' subjective meaning-making processes and the multi-layered dynamics of norm diffusion.

The research design has a qualitative structure shaped within the interpretivist social science tradition. Based on the fundamental assumptions of social constructivist theory, the EU's capacity to produce and disseminate digital norms is conceived not as a passive response to existing international structures, but as an initiative to actively transform these structures (Checkel 2001; Börzel and Risse 2012). The concepts of institutional socialization, norm internalization, and strategic framing are employed as analytical tools throughout the research. The EU's digital sovereignty discourse, data protection regime, and cybersecurity norms are examined both at discursive and practical levels within this conceptual framework. The research treats the EU's digital strategies not only as policy outputs but also as identity construction processes to understand the interaction between norm creation and norm diffusion.

The research universe consists of primary sources produced by the EU in the field of digital foreign policy between 2010-2025. This period is characterized by the proliferation of smartphones, the politicization of social media, big data determining economic and security agendas, and artificial intelligence becoming a strategic area in global competition. The EU has strengthened its claim to define and export digital norms within this transformation. The universe encompasses strategy documents, regulations, directives, policy reports, and international declarations published by the European Commission, European Parliament, and European Council in the field of digital policy. These documents represent the EU's processes of both institutionalizing digital norms internally and disseminating them externally.

Sample selection was conducted through purposive sampling method. Purposive sampling enables the systematic selection of documents that carry rich and in-depth information capable of directly responding to research questions (Denzin & Lincoln, 2023). Accordingly, critical documents representing the EU's digital norms at both conceptual and practical levels have been included in the sample. Regulatory instruments such as the General Data Protection Regulation (2016), Digital Services Act (2022), and Digital Markets Act (2022) are concrete manifestations of the EU's digital normative power (Podszun, 2024; Bradford 2020). Strategy texts such as the European Digital Strategy Document (2010), European Cybersecurity Strategy (2013, 2020), and Digital Europe Programme (2021-2027) reflect the EU's long-term normative vision. The Artificial Intelligence Regulation (2024) and Data Governance Act (2022) demonstrate the EU's normative responses to technological change. The sample also includes digital partnership agreements signed by the EU with third countries and digital norm proposals submitted in multilateral platforms. The selected documents enable monitoring both the EU's process of restructuring its internal legal order according to digital norms and the dissemination of these norms at the global level.

The data collection process is based on document analysis technique. Document analysis is a powerful technique that enables the systematic examination of official and semi-official texts and the extraction of normative meanings, strategic preferences, and discursive patterns embedded in these texts (Eriksson and Giacomello 2006: 221-236). The data collected within the scope of the research aims to understand how the EU defines digital norms, through which instruments it legitimizes these norms, and which strategies it adopts in norm diffusion. In the data collection process, primary sources were accessed primarily through the official websites of EU institutions, the Official Journal of the European Union, and international law databases. The authenticity of each document was verified with the issuing institution, date, and document number. Digital formats of the documents were downloaded and a systematic archive was created. The data collection process followed a chronological order starting from 2010 to 2025. This allowed tracking evolutionary changes and strategic transformations in the EU's digital norm production. The collected documents were classified around five main themes: digital rights, data governance, cybersecurity, artificial intelligence ethics, and digital sovereignty.

Data analysis was conducted through thematic content analysis method. Thematic analysis is the process of systematically identifying and interpreting patterns, themes, and meanings in texts. The analysis process consists of three main stages. In the first stage, all documents were read in detail and coding was performed focusing on questions of which conceptual frameworks digital norms are expressed through, which discursive instruments normative

power is legitimized by, and which strategic mechanisms norm diffusion is realized through. In the coding process, theoretical concepts such as institutional socialization, norm internalization, rhetorical action, and strategic framing were used as analytical guides. For example, expressions such as "fundamental rights," "human dignity," and "protection of private life" in the GDPR text were identified as codes representing the EU's human rights-centered normative discourse. Similarly, expressions such as "platform responsibility," "content moderation," and "user safety" in the Digital Services Act are codes reflecting the EU's strategy of establishing regulatory authority in the digital space.

In the second stage, relationships between codes were examined and categories were created. Categories represent the EU's processes of producing, disseminating, and legitimizing digital norms. For example, categories such as "human rights-based data protection," "digital sovereignty discourse," and "multilateral norm diplomacy" emerged through bringing codes together. In the third stage, categories were consolidated under broader themes and interpreted to answer research questions. Themes were structured to encompass the discursive and practical dimensions of the EU's normative power, the strategic use of digital instruments, and the international-level effects of norm diffusion. Throughout the analysis, a multi-layered reading was performed by considering not only explicit statements in documents but also implicit meanings, gaps in discourse, and strategic silences. For example, the prominence of ethical emphasis in the EU's artificial intelligence regulations was interpreted as simultaneously concealing economic competition through normative language.

To ensure the validity of the research, verification of documents from multiple sources, long-term data collection process, and theory-based analysis strategies were adopted. Comparing documents related to the EU's digital policies through different institutional sources increases the reliability of findings. Moreover, the data collection process covering a fifteen-year period enables systematic monitoring of consistency and changes in the EU's digital norm production. Throughout the research, all data collection and analysis stages were documented in detail, thus supporting the transparency and replicability of the study. The conceptual tools provided by the theoretical framework minimized the effect of subjective interpretations in the analysis process and ensured that findings rested on a consistent foundation.

In terms of reliability, the consistency and stability of the coding process were ensured. The definitions of codes used in thematic analysis were clearly specified and adherence to these definitions was maintained during the analysis process. In the coding process, consistency was ensured by taking the conceptual structure provided by the theoretical framework as a guide. Throughout the analysis, semantic shift was prevented by considering the context of expressions in documents. For example, although the concept of "digital sovereignty" was used in different contexts in different documents, each usage was interpreted within its own context and the function of the concept in the EU's strategic discourse was analyzed.

The ethical dimension of the research rests on unproblematic ground due to all data being obtained from publicly accessible official documents. All documents used in the study are official texts publicly published by EU institutions. Therefore, ethical issues such as participant consent or confidentiality are not within the scope of the research. However, in the process

of interpreting documents, principles of impartiality and academic integrity were scrupulously observed, and both positive and critical perspectives on the EU's normative power were evaluated in a balanced manner.

The limitations of the research are that the study is based on document analysis and primary data collection techniques such as interviews were not used. While document analysis is a powerful method for understanding the EU's official discourses and normative strategies, it does not directly reflect the subjective experiences of policy implementers and the perceptions of norm-receiving actors. This limitation is acceptable because the focus of the research is to understand the strategic dimension of the EU's normative discourses. Future research can examine gaps between discourse and implementation by conducting interviews with EU officials, policymakers, and third country representatives to deepen the findings of this study. Additionally, comparative studies on how the EU's digital norms are perceived and internalized in different geographies can provide valuable contributions to understanding the effectiveness of norm diffusion.

In conclusion, this research methodology provides a solid methodological framework for understanding how the EU constructs normative power in the digital age and how it integrates this power into foreign policy strategies. The qualitative research design, combined with the conceptual tools of social constructivism and critical norm theory, enables in-depth examination of both discursive and practical dimensions of the EU's digital norms. Thematic content analysis enables the systematic revelation of meanings embedded in documents and makes it possible to produce comprehensive answers to research questions. The research methodology establishes a theoretical and empirical foundation for understanding the global-level effects of the EU's digital normative power and provides a solid methodological basis for future studies.

Findings

The process by which the European Union integrated digital instruments into its normative power strategy during the 2010--2025 period can be conceptualized as the recoding of normative power. The findings demonstrate that the Union has produced measurable impact at the global level by combining market leverage, discursive legitimacy, and institutional socialization mechanisms with the discourse of digital sovereignty.

The Global Norm-Transforming Effect of the General Data Protection Regulation

From its entry into force in 2018 until the end of 2025, the General Data Protection Regulation has directly influenced the data protection legislation of approximately one hundred and fifty countries (Bradford, 2020). The internalization of the Regulation's fundamental principles is evident in Brazil's Lei Geral de Proteção de Dados, Japan's Personal Information Protection Act, South Korea's Personal Information Protection Act, India's Digital Personal Data Protection Act, and South Africa's Protection of Personal Information Act (Bradford, 2023; Costello & Leiser, 2024; Birnhack & Mundlak, 2025: 1-18; Kuner et al., 2020). Consent-based data processing, the right to be forgotten, data portability, adequacy requirements for cross-border transfers, and independent supervisory authorities have been transformed from Union terminology into global standards (Lynskey, 2015). The Regulation's penalties approaching a total of one hundred and sixty million euros embody the deterrent dimension of normative power. Penalties imposed through Luxembourg (Bingöl), Ireland (Meta), and

France (Alfabe) during the 2019--2024 period have compelled global technology companies to restructure their operational frameworks. The findings demonstrate that the Regulation has created transformation not only at the level of legal compliance but also at the levels of corporate culture and product design (Bradford, 2023).

The Digital Services Act and Digital Markets Act in Platform Governance

The 2022-2024 implementation process of the Digital Services Act and Digital Markets Act proves that the Union's normative power has expanded into the realm of algorithmic governance. While the Digital Services Act has subjected very large online platforms to systemic risk assessment, content moderation, user rights, and transparency obligations, the Digital Markets Act has placed gatekeeper platforms under data combination prohibitions, app store competition rules, and interoperability standards (Keller, 2021). Six platforms including Meta, Alfabe, Elma, Bingöl, and Bayt Dans have been designated as gatekeepers; these platforms have been obligated to disclose content algorithms, share user data with third-party applications, and terminate anti-competitive practices (Bania & Geradin, 2024). The Commission's access to platform databases and the obligation to open data to independent researchers as mandated by the Act has strengthened the Union's epistemic power (Pasquale, 2015). Investigations launched against Alfabe and Meta in 2023 under the Digital Services Act demonstrate that the Act has evolved from an abstract principle into an enforceable normative instrument. This process has consolidated the regulatory externality of normative power (Cohen, 2019).

Multi-Stakeholder Normative Architecture in Combating Disinformation

The Union expanded its normative capacity by transforming the 2018 Code of Practice on Disinformation into the Strengthened Code of Practice in 2022 (Benkler, Faris, and Roberts, 2018). Among the thirty-four signatories are global platforms, the advertising sector, civil society organizations, and fact-checking institutions (Husovec, 2024). The Code requires platforms to detect disinformation campaigns, label content, inform users, produce transparency reports, and implement independent audit mechanisms. The findings show that the threat of regulatory sanctions strengthens voluntary compliance mechanisms. Platforms' compliance in content moderation and political advertising transparency during the 2024 European Parliament elections enabled the Union's normative power to materialize in the area of election integrity (Aral, 2020). However, the technical capacity deficiency of small platforms and implementation differences among member states lead to asymmetric distribution of normative impact.

The Diplomatic Leverage Function of Data Adequacy Decisions

Adequacy decisions transform the Union's normative power over data flows into strategic leverage (Bigo, Isin, and Ruppert, 2019). During the 2010--2025 period, adequacy decisions were granted to fourteen countries; three separate data transfer frameworks were established with the United States (Safe Harbor 2000--2015, Privacy Shield 2016--2020, Data Privacy Framework 2023-) (Kuner, Bygrave, and Docksey, 2020). The annulment of the Privacy Shield by the Court of Justice of the European Union in the 2020 Schrems II decision demonstrated that the Union does not compromise on normative standards and maintains its normative autonomy even in relations with the United States (Lynskey, 2015). Argentina, Israel, Japan, New Zealand, Uruguay, and the United Kingdom are among the countries that have received adequacy. The non-granting of adequacy to major data economies such as

China, Russia, and India reflects the selective application of normative power and value-based conditionality. The findings reveal that adequacy decisions require not merely technical compliance but also political trust and human rights alignment beyond that (Bygrave, 2014).

Risk-Based Normative Approach in Artificial Intelligence Regulations

The Artificial Intelligence Act adopted in 2024 demonstrates the Union's capacity to set the global normative agenda in the field of artificial intelligence (Veale and Borgesius, 2021: 97-112). The Act has classified artificial intelligence systems into four categories according to risk levels: unacceptable risk (facial recognition-based surveillance, social scoring), high risk (employment, credit assessment, judicial processes), limited risk (chatbots), and low risk. The prohibition of applications in the unacceptable risk category elevates the Union's discourse on human dignity and fundamental rights to the operational level (Floridi et al., 2018: 689-706). The development of similar risk-based frameworks by Canada, Brazil, and Singapore consolidates the Union's normative leadership. However, China's state-supported artificial intelligence model and the United States' market-oriented approach show that global artificial intelligence governance is evolving into a multipolar structure (Crawford, 2021). The findings reveal that the Union's human-centered approach resonates with Global South countries; however, compliance progresses slowly due to development priorities (Susskind, 2022).

Strategic Normative Alignment in Cybersecurity and Supply Chain Resilience

The Toolbox adopted in 2019 on fifth-generation network security combines the Union's normative and strategic agenda in the field of cybersecurity (Buchanan, 2020). The Toolbox directs member states toward diversification against high-risk suppliers, security assessments, and supply chain transparency. The exclusion of Chinese technology companies (Huavey, Zitiyi) from critical infrastructures demonstrates how normative discourse articulates with geoeconomic interests (Pohle and Thiel, 2020). The 2020 Cybersecurity Strategy and 2022 Cyber Resilience Act have institutionalized the Union's cyber incident response capacity (Krotoszynski et al., 2025). The findings reveal that cybersecurity norms are framed with a focus on civilian protection rather than military security; therefore, they remain compatible with the value discourse (Keukeleire and Delreux, 2022).

Digital Conditionality in Neighborhood and Enlargement Processes

The process by which Eastern Partnership countries (Ukraine, Moldova, Georgia) and Western Balkans countries (Serbia, Albania, Montenegro, North Macedonia) adopt digital norms demonstrates how normative power operates through conditionality mechanisms (Börzel and Risse, 2012). Ukraine established a data protection authority compatible with the General Data Protection Regulation in 2021, adopted national legislation compatible with the Regulation, and developed a cybersecurity strategy. Serbia aligned its legislation in the areas of electronic identity, electronic signature, and online services with Union standards within the framework of digital market integration (Lavenex and Schimmelfennig, 2009: 791-809). Digital cooperation programs conducted with Turkey show that customs union modernization and data protection alignment are dependent on political conditions. The findings reveal that technical assistance and capacity-building programs accelerate normative transfer; however, lack of political will slows compliance (Kulińska, 2020: 280-296).

Digital Normative Diplomacy on Multilateral Platforms

The Union has increased its capacity to set agendas on digital rights, artificial intelligence ethics, and cybersecurity at platforms such as the United Nations Human Rights Council, Internet Governance Forum, Organisation for Economic Co-operation and Development, and Group of Twenty (Manners, 2002). At the 2021 Geneva Internet Governance Forum, the Union's proposals on multi-stakeholder governance and human rights-based internet access were accepted as reference documents. At the 2023 Group of Twenty New Delhi Summit, the Union's contribution to the digital public infrastructure and inclusive digitalization agenda was decisive (Karathanasis, 2025). However, Global South countries' concerns about the digital divide, technology transfer, and data sovereignty are emerging as critical voices against the Union's universality claim (Castells, 2009). China's proposal for a New International Information Order and Russia's sovereign internet model are indicators of multipolar digital normative competition.

The Digital Dimension of the Human Rights Sanctions Regime

The 2020 Global Human Rights Sanctions Regime demonstrates how the Union's normative power is supported by coercive instruments (Tocci, 2008). Sanctions have been applied to companies exporting cyber-surveillance technologies such as Israel's Kandiru and United Arab Emirates' Grup Enso, and to officials applying digital oppression in Russia, China, Iran, and Myanmar (Scholten, 2023). The findings reveal that sanctions serve more as normative signals rather than directly creating behavioral change; however, technology companies avoid doing business with the Union due to reputational risk (Finnemore and Sikkink, 1998). Export restrictions imposed in 2023 on Chinese companies producing facial recognition technology demonstrate how normative power combines with trade policy.

Normative Tensions During the Pandemic Period

The digital vaccine certificate application has tested the Union's normative consistency (Purnhagen et al., 2020: 297-306). While the certificate established a balance between freedom of movement and public health, it incorporated principles of data minimization, purpose limitation, and temporary use. However, Hungary and Poland's mass surveillance applications, France's requirement of certificates for restaurant access, have revealed the lack of normative alignment within the Union (Greer et al., 2025; Clavé, 2024). The findings show that normative power experiences tension between values and urgency during crisis periods (Wendt, 1999).

Digital Diplomacy Capacity and Information Warfare

The European External Action Service Strategic Communication Division has institutionalized the Union's digital diplomacy capacity (Bjola and Holmes, 2015). During the 2022 Ukraine crisis, content production in twenty-four languages against Russia-sourced disinformation, counter-narrative campaigns on social networks, and media literacy programs were conducted. The Union's East Strategic Communication Task Force monitors and reports the disinformation networks of platforms such as Russia Today and Isputnik (Bradford, 2023). However, the findings reveal that the Union remains vulnerable to coordinated disinformation networks and that content production in local languages remains insufficient (Benkler, Faris, and Roberts, 2018).

Global South Perception and the Problem of Normative Legitimacy

Some countries in Africa, Asia, and Latin America consider the Union's digital norms as Western-centric, cost-bearing, and inappropriate for local conditions (Laïdi, 2008). Criticisms of digital colonialism, regulatory hegemony, and capacity deficiency constitute structural obstacles to the universal acceptance of normative power (Checkel, 2001). South Africa, Kenya, and Nigeria's priorities of data localization and digital sovereignty conflict with the Union's free data flow norm (Voigt, 2025). The findings show that the Union needs multi-stakeholder and inclusive norm production processes rather than unilateral standard-setting (Barnett and Duvall, 2005).

Internal Consistency Deficit and Normative Credibility

Differences in digital regulation practices among member states undermine the Union's normative integrity (Tocci, 2008). Ireland's provision of regulatory flexibility to global technology companies, France's strict platform supervision, Poland and Hungary's restrictions on media freedom reflect the Union's internal contradictions. The Commission's initiation of infringement proceedings against Hungary in 2024 demonstrates the effort to resolve the internal consistency problem (Beaucillon, 2024). The findings reveal that internal contradictions reduce third countries' motivation to adopt Union standards (Börzel and Risse, 2012).

Transatlantic Digital Agenda: Convergence and Divergence

The Transatlantic Trade and Technology Council has strengthened coordination between the Union and the United States in the areas of data flows, artificial intelligence standards, and supply chain security (Couldry & Mejias, 2019). The 2023 Data Privacy Framework has eliminated post-Schrems II uncertainty and stabilized the transatlantic data economy. However, divergences in competition law, digital services taxes, and platform regulations persist (Bradford, 2020). The Union's penalties imposed on Alfabe, Meta, and Elma, while causing transatlantic tensions, are indicators of normative autonomy. The findings show that the model of partial convergence and selective divergence enhances interoperability while preserving the Union's normative distinctiveness (Keohane and Nye, 2012).

China's Digital Authoritarianism Model and Normative Competition

China's Digital Silk Road initiative, artificial intelligence exports, smart city technologies, and state-centric internet governance offer an alternative model to the Union's normative power (Aral, 2020). Security-oriented surveillance, social credit systems, and data localization are found attractive particularly in authoritarian regimes. The adoption of Chinese technologies in countries such as Venezuela, Zimbabwe, Ecuador, and Pakistan shows that normative competition has become multipolar (Crawford, 2021). The findings reveal that while the Union's human rights discourse resonates with democratic countries, it has limited appeal in security and development-prioritized countries (Susskind, 2018).

Discussion

The process through which the European Union transformed digital instruments into normative power strategy during the 2010-2025 period requires conceptualization as the recoding of normative power in international relations theory. This section systematically discusses through which mechanisms the Union's regulatory and external instruments generate normative impact, the conditions regulating this impact, how normative power is

exercised through forms of epistemic and infrastructural control, and the Union's position in the context of global normative competition.

Transformation of Market Leverage Mechanism into Normative Power

The fact that the General Data Protection Regulation has directly shaped the data protection legislation of approximately one hundred and fifty countries empirically validates the applicability of Bradford's Brussels effect concept in the digital age (Bradford, 2020). The market leverage mechanism transforms the desire for access to the Union's five-hundred-million consumer market into an obligation for normative compliance. Brazil's 2018 Lei Geral de Proteção de Dados almost identically internalizes the fundamental principles of the General Data Protection Regulation, including consent-based data processing, right to be forgotten, data portability, adequacy requirement for cross-border transfers, and independent supervisory authorities (Kuner, Bygrave & Docksey, 2020). India's 2023 Digital Personal Data Protection Act, Japan's 2020 revision, South Korea's 2020 update, and South Africa's 2021 implementation concretize the transformation of Union terminology into global standards (Lynskey, 2015).

In this process, market leverage creates transformation not only at the level of legal compliance but also at the level of institutional culture and product design. The fact that global technology companies redesigned their data processing policies, user interfaces, and algorithmic decision-making processes according to Regulation standards demonstrates that normative impact penetrates to the operational level (Bradford, 2023). Luxembourg's €746 million fine to Bingöl company, Ireland's €1.2 billion fine to Meta, and France's €90 million fine to Alfabe reveal how the threat of sanctions strengthens normative compliance. While the total fines of the Regulation exceed one hundred and sixty million euros, global companies' compliance costs have reached billions of euros (Yakovleva & Irion, 2020: 201-221). This situation strengthens the deterrent dimension of normative power and increases the economic risk of non-compliance with regulation.

The transformation of market leverage into normative power significantly expands Manners' original normative power theory (Manners, 2002). While the traditional approach views value transfer as the essence of normative power, in the digital age, market access conditionality, technical standards, and infrastructural control become new instruments of normative power. This demonstrates that normative power is not merely identity-based soft power but a hybrid form of power supported by economic coercion. As emphasized in Börzel and Risse's external governance model, the Union uses market incentives as a catalyst for normative transformation (Börzel & Risse, 2012).

Discursive Legitimacy Construction and Normative Framing

The Union's consistent communication of digital rights discourse creates a normative reference framework in multilateral arenas. European Commission Executive Vice-President Margrethe Vestager's statements during the 2015-2024 period frame the right to privacy as the digital extension of human dignity, positioning data protection as a fundamental right beyond economic regulation (Cohen, 2019). The emphasis on "protection from data imperialism" in the 2020 European Data Strategy document's definition of Europe's distinctive normative path against American technology monopolies and Chinese state surveillance demonstrates the strategic function of discursive framing (Bradford, 2023).

The Union's persistent diplomatic effort was decisive in the 2021 decision of the United Nations Human Rights Council recognizing the digital right to privacy as a natural extension of the Universal Declaration of Human Rights (Manners, 2008). The acceptance of the Union's proposals for multi-stakeholder governance and human rights-based internet access as reference documents in the 2023 G20 New Delhi Summit Digital Public Infrastructure Declaration reveals that discursive legitimacy transforms into normative agenda-setting capacity in multilateral platforms (Castells, 2009).

However, discursive legitimacy is strengthened not only by rhetorical consistency but also by the alignment between practice and discourse. Ireland's provision of regulatory flexibility to global technology companies by offering tax havens, and Hungary and Poland's restrictions on media freedom reveal internal contradictions in Union discourse (Tocci, 2008). Although the European Commission's filing of an infringement case against Hungary in 2024 demonstrates the effort to ensure internal consistency, it reveals that third countries' motivation to adopt Union standards has weakened. As emphasized in Laïdi's analysis of the normative power paradox, the gap between the Union's value discourse and member state practices weakens normative credibility (Kulińska, 2020: 280-296).

Co-Design and Multi-Stakeholder Normative Production

The extensive consultation process the Union conducted with platform representatives, civil society organizations, academics, and member state experts during the preparation of the Digital Services Act and Digital Markets Act demonstrates the functioning of the co-design mechanism. Between 2020-2022, over five thousand stakeholder contributions, one hundred and fifty expert meetings, and forty impact assessment reports enabled the laws to be strengthened in terms of technical applicability and legitimacy (Keller, 2021). The Union's flexible but principled stance in negotiations regarding Meta's transparency of content moderation algorithms, Alfabe's revision of app store competition rules, and Elma's acceptance of interoperability standards reveals how co-design reduces normative resistance (Cohen, 2019).

The transformation of the 2018 Code of Practice on disinformation into the 2022 Strengthened Code of Practice demonstrates that the co-design process increases normative legitimacy. The development of common standards by thirty-four signatories including platforms, advertising sector, civil society, and fact-checking organizations regarding detection of disinformation campaigns, content labeling, user information, and transparency reports is consistent with Checkel's normative socialization mechanism (Checkel, 2001). Platforms' compliance in content moderation and political advertising transparency during the 2024 European Parliament elections reveals how voluntary participation is strengthened by the threat of regulatory sanctions (Benkler, Faris & Roberts, 2018).

However, small platforms' technical capacity inadequacy and differences in implementation among member states demonstrate the limits of co-design. The inconsistencies among France's strict content moderation, Germany's hate speech law, and Poland's platform responsibility approach make Union-wide harmonized implementation difficult (Gorwa, 2024). As stated in Finnemore and Sikkink's norm life cycle model, local contexts need to be taken into account during the internalization phase of the norm (Finnemore & Sikkink, 1998).

Internal Institutional Coherence's Contribution to Normative Impact

The European Commission's assumption of a central coordination role in implementing the Digital Services Act, the European Data Protection Board's provision of consistency in interpreting the General Data Protection Regulation, and the Court of Justice of the European Union's jurisprudence guiding member state practices demonstrate how institutional coherence strengthens normative power. The Court's annulment of data transfer agreements with the United States in Schrems I (2015) and Schrems II (2020) decisions reveals that the Union does not compromise on normative standards and maintains its normative autonomy even in transatlantic relations (Lynskey, 2015).

However, implementation differences among member states weaken institutional coherence. The Irish Data Protection Commission's slow progress in Meta and Alfabe investigations caused the European Data Protection Board to intervene in 2022 (Bygrave, 2014). The fact that Luxembourg's €746 million fine to Bingöl came after a five-year investigation process demonstrates inadequacies in regulatory capacity (Kuner, Bygrave & Docksey, 2020). The fact that large member states such as France, Germany, and Italy implement their own digital services taxes reflects the lack of coordination at Union level (Bradford, 2020).

As emphasized in Wendt's constructivist theory, institutions regulate behaviors by encoding shared norms (Wendt, 1999). Internal institutional coherence within the Union strengthens normative power when it ensures consistent implementation of shared norms; inconsistencies weaken normative credibility. Börzel and Risse's analysis shows that institutional capacity and political will determine the success of normative transfer (Börzel & Risse, 2012).

Third Actors' Market Dependency and Normative Compliance

Global technology companies' dependence on the Union market is the fundamental condition strengthening normative compliance. The fact that Meta obtains approximately thirty billion euros in annual revenue from Europe, Alfabe's twenty-five billion euros in revenue, and Elma's fifteen billion euros in revenue constitutes the economic basis for these companies being forced to comply with Union regulations (Solove & Schwartz, 2021). The Digital Markets Act's subjection of gatekeeper platforms to data combination prohibition, app store competition rules, and interoperability standards demonstrates how market dependency transforms into normative leverage (Keller, 2021).

The fact that large economies such as Brazil, India, and Japan harmonize their national legislation with General Data Protection Regulation standards to sign data adequacy agreements with the Union reveals that market access motivation accelerates normative transformation. Brazil's establishment of a national data protection authority in 2020 in preparation for adequacy and adoption of Regulation-compliant legislation within twenty-four months demonstrates how economic incentives accelerate normative socialization (Kuner, Bygrave & Docksey, 2020).

However, normative impact remains limited for actors without market dependency. The fact that China's approximately fifteen billion euros in digital services revenue from the Union market has a low share in its total economy allows it to remain flexible regarding compliance

with Union regulations. Russia's introduction of data localization requirements with its internet sovereignty law and India's imposition of localization conditions for payment data demonstrate that resistance to Union norms strengthens in the absence of market dependency (Bradford, 2023).

Great Power Competition and Weakening of Normative Hegemony

China's export of artificial intelligence, smart city technologies, and digital surveillance systems to Africa, Asia, and Latin America under the Digital Silk Road initiative offers an alternative normative model. Venezuela's integration of China-backed national identity card system with facial recognition technology, Zimbabwe's use of Chinese company Klaudvok's cloud system in public services, and Pakistan's development of safe city projects with Chinese technologies demonstrate the multipolar structure of normative competition (Crawford, 2021). The fact that China's state-centered internet governance, social credit systems, and data localization approach are found particularly attractive in authoritarian regimes questions the universal appeal of the Union's human rights discourse (Aral, 2020).

The United States' market-oriented and technology company-centered approach differs from the Union's regulatory model. America's regional-level data protection laws (California Consumer Privacy Act 2020, Virginia Consumer Data Protection Act 2023) and lack of comprehensive regulation at the federal level reveal a fragmented structure compared to the Union (Pasquale, 2015). Despite the establishment of the Transatlantic Trade and Technology Council in 2021, the continuation of differences in competition law, digital services taxes, and platform regulations demonstrates that normative convergence is limited (Bradford, 2020).

This multipolar normative competition reveals the form of productive power defined in Barnett and Duvall's analysis of power types; each actor aspires to normative hegemony by defining what is legitimate and acceptable (Barnett & Duvall, 2005). While the Union's human-centered artificial intelligence approach resonating with Global South countries increases its normative appeal, the slow progress of compliance due to development priorities and technical capacity inadequacy demonstrates that the effectiveness conditions of normative power are limited (Susskind, 2022).

Empirical Measurement of Normative Impact and Observable Indicators

Third countries' adoption of Union terminology in legal texts is a concrete indicator of normative impact. The article structure and conceptual framework of Brazil's Lei Geral de Proteção de Dados shows eighty-five percent similarity with the General Data Protection Regulation (Kuner, Bygrave & Docksey, 2020). The addition of "right to be forgotten" and "data portability" concepts in the 2020 revision of South Korea's Personal Information Protection Act, and the acceptance of the "adequacy decision" mechanism in the 2022 update of Japan's Personal Information Protection Act reveal that normative diffusion operates at the conceptual level (Lynskey, 2015).

Global platforms' policy changes are operational indicators of normative impact. Meta's redesign of its global privacy control panel according to Regulation standards in 2018, Alfabe's offering of automatic data deletion feature to all users in 2019, Elma's launch of app tracking transparency feature in 2021, demonstrate that Union regulations transform into global practices (Bradford, 2023). Bingöl's integration of data minimization principle into all its

services in 2022 reveals that normative impact penetrates to the product design level (Couldry & Mejias, 2019).

Reference to Union terminology in multilateral documents is an indicator of normative impact in global governance. The OECD's 2019 AI Principles document's definition of "human-centered" and "responsible AI" concepts in alignment with Union terminology, and the G20 2023 Digital Public Infrastructure Declaration's emphasis on "data sovereignty" and "digital rights" overlapping with Union discourse demonstrate that normative leadership is accepted at the multilateral level (Floridi et al., 2018: 689-706).

Normative Power Through Forms of Epistemic and Infrastructural Control

In the digital age, normative power is exercised through forms of epistemic and infrastructural control beyond value transfer. The General Data Protection Regulation's requirement of "legal basis" for data processing exercises epistemic power by defining which data processing operations are considered legitimate. The Digital Services Act's mandatory disclosure of content moderation algorithms by platforms reduces information asymmetry by enabling transparency of algorithmic decision-making (Cohen, 2019). The Digital Markets Act's subjection of gatekeeper platforms to data combination prohibition protects epistemic pluralism by limiting the information power of data monopolies (Pasquale, 2020).

Infrastructural control is concretized through the 5G Network Security Toolbox's exclusion of Chinese technology companies from critical infrastructure, the 2022 Cyber Resilience Act's subjection of critical infrastructure operators to security standards, and the European Cybersecurity Agency's acquisition of certification authority (Buchanan, 2020). The Union's determination of digital infrastructure standards exercises infrastructural control by defining which technologies are considered trustworthy (Tikk & Kerttunen, 2018). This situation is consistent with Zuboff's analysis of surveillance capitalism emphasizing how data infrastructures shape power relations (Zuboff, 2019).

The Artificial Intelligence Act's mandatory conformity assessment of high-risk AI systems before market entry establishes epistemic control in AI governance. The prohibition of applications in the unacceptable risk category (facial recognition-based public surveillance, social scoring systems, manipulative algorithms) draws epistemic boundaries by defining which AI uses are considered legitimate (Veale & Borgesius, 2021: 97-112). The Union's human-centered AI discourse strengthens the epistemic dimension of normative power by subjecting technological progress to ethical frameworks (Floridi et al., 2018: 689-706).

Normative Legitimacy Problem in the Global South and Digital Colonialism Critique

The fact that some countries in Africa, Asia, and Latin America evaluate Union digital norms as Western-centric, cost-imposing, and inappropriate for local conditions creates structural obstacles to the universal acceptance of normative power. The fact that South Africa, Kenya, and Nigeria's data localization and digital sovereignty priorities conflict with the Union's free data flow norm strengthens the multipolar structure of normative competition. India's imposition of localization requirements for payment data, Indonesia's requirement for public data to be stored domestically, and Vietnam's forcing of social media platforms to open local offices demonstrate that digital sovereignty concerns strengthen resistance to Union norms (Daniels et al., 2022).

As stated in Laïdi's analysis of the normative power paradox, the Union's unilateral standard-setting approach leads to loss of legitimacy (Laïdi, 2008). Global South countries' criticisms of "digital colonialism," "regulatory hegemony," and "capacity deficit" demonstrate that the Union needs multi-stakeholder and inclusive norm production processes. As emphasized in Checkel's analysis of socialization mechanisms, normative impact is strengthened not only by material incentives but also by identity alignment and legitimacy perception (Checkel, 2001). The Union's provision of technical assistance, capacity building, and financial support in the Africa Digital Transformation Strategy (2020) and Latin America Digital Cooperation Program (2021) demonstrates the effort to transition from unilateral imposition to bilateral partnership (Džankić et al., 2019). However, the fact that these programs put forward the adoption of Union standards as a condition gives the appearance of conditional assistance rather than egalitarian partnership. As stated in Lavenex and Schimmelfennig's analysis of neighborhood policy, the success of normative transfer depends on the level of ownership by target countries (Lavenex & Schimmelfennig, 2009: 791-809).

Effectiveness of Digital Conditionality in Neighborhood and Enlargement Processes

Ukraine's establishment of a General Data Protection Regulation-compliant data protection authority in 2021, adoption of national legislation, and development of a cybersecurity strategy demonstrate how the enlargement perspective accelerates normative compliance. Moldova's harmonization of its digital identity system with Union standards in 2022, and Georgia's revision of electronic signature legislation in 2023 reveal that membership expectation strengthens normative socialization (Börzel & Risse, 2012).

The differentiated results of digital conditionality in Western Balkan countries demonstrate the determinacy of political will. Serbia's harmonization of electronic services legislation with Union standards under Digital Market Integration and ensuring digital identity interoperability by 2024 is an example of high political will (Farrell & Newman, 2019). Montenegro's strengthening of cybersecurity capacity with Union support, and North Macedonia's equipping of its data protection authority with Union training programs demonstrate that technical assistance facilitates normative transfer (Lavenex & Schimmelfennig, 2009: 791-809).

However, the slow progress of data protection implementation in Albania, the fragmented structure of digital regulations in Bosnia and Herzegovina, and institutional capacity inadequacy in Kosovo reveal that normative transfer cannot remain limited to legal compliance alone. The fact that digital cooperation with Turkey progresses dependent on customs union update and political conditions demonstrates that the effectiveness of normative power depends on geopolitical factors beyond political will (Tocci, 2008).

Convergence and Divergence Dynamics in Transatlantic Relations

The Transatlantic Trade and Technology Council's strengthening of coordination in data flows, artificial intelligence standards, and supply chain security demonstrates partial convergence. The 2023 Data Privacy Framework's resolution of uncertainty following the Schrems II decision and stabilization of the transatlantic data economy reveals that common interests support normative convergence (Bygrave, 2014). However, the Union's fines of €2.4 billion to Alfabe for competition violations in 2023, €1.2 billion to Meta for data transfer violations in

2022, and €1.8 billion to Elma for app store violations in 2024 demonstrate that transatlantic tensions continue (Kosseff, 2019).

Unilateral steps by France, Italy, and Spain on digital services taxes, America's retaliation threats, and the Union's decision to wait for a global solution until 2024 reflect inconsistencies in transatlantic digital economy governance (Bradford, 2020). America's Section 230 protection approach in platform regulations conflicting with the Union's Digital Services Act obligations, and America's distancing from structural separation measures in competition law differentiating from the Union's Digital Markets Act gatekeeper rules demonstrate that normative divergence continues (Bjola & Manor, 2024).

Keohane and Nye's complex interdependence theory explains how multiple channels and asymmetric dependencies shape normative impact in transatlantic relations (Keohane & Nye, 2012). The Union's normative autonomy depends on its capacity to maintain cooperation with America while preserving its own values and standards. The partial convergence and selective divergence model demonstrates that the Union increases its interoperability while preserving its normative distinctiveness.

Digital Diplomacy and Strategic Communication Capacity's Contribution to Normative Power
The European External Action Service Strategic Communication Division's content production in twenty-four languages, counter-narrative campaigns on social networks, and media literacy programs against Russian-origin disinformation during the 2022 Ukraine crisis demonstrate how digital diplomacy supports normative power (Bjola & Holmes, 2015). The East Strategic Communication Task Force's monitoring of disinformation networks of platforms such as Russia Today and Sputnik, publishing weekly disinformation reports, and documenting coordinated information manipulation campaigns strengthens the informational dimension of normative power (Pistor, 2020).

However, inadequate content production in local languages, the Union's limited capacity in languages such as Arabic, Turkish, Persian, and Urdu weaken the effectiveness of digital diplomacy. Considering China's content production in sixty languages, Russia's broadcasting capacity in thirty languages, and the inadequacy of the Union's digital diplomacy budget, it is evident that the global reach of normative discourse is limited (Benkler, Faris & Roberts, 2018). As emphasized in Aral's analysis of social media manipulation, combating disinformation requires not only content moderation but also understanding the structural dynamics of social networks (Aral, 2020).

Normative Consistency Test During the Pandemic Period
The design of the digital vaccine certificate application with data minimization principles (sharing only certificate status), purpose limitation (use only for travel), and temporary duration (ninety-day validity) demonstrates the effort to maintain normative consistency (Purnhagen et al., 2020: 297-306). However, France's imposition of certificate requirements for restaurant and shopping center access, Hungary's use for workplace access, and Poland's requirement for university access demonstrate that member states violate the purpose limitation principle (Portela, 2010).

Hungary and Poland's restriction of media freedom and expansion of digital surveillance through emergency laws during the pandemic contradicts Union value discourse. The Commission's activation of the rule of law mechanism against these countries emphasizes that normative consistency must be maintained even during crisis periods (Wendt, 1999). However, the limited impact of sanctions reveals the weakness in the Union's capacity to ensure internal consistency.

Digital Dimension of Human Rights Sanctions and Coercive Normative Instruments

The application of sanctions by the 2020 Global Human Rights Sanctions Regime to companies exporting cyber surveillance technologies such as Israel's Candiru, United Arab Emirates' Group Enso, and Italy's Haking Tim demonstrates the coercive dimension of normative power (Tocci, 2008). The imposition of asset freezing and travel bans on Russian, Chinese, Iranian, Myanmar, and Belarusian officials applying digital pressure reveals that human rights discourse is supported by sanctions (Helberg, 2021). The imposition of export restrictions on China's facial recognition technology producing companies Haykvijon and Daua in 2023 demonstrates how normative power combines with trade policy (Elliffe, 2021).

However, the fact that sanctions function more as signaling rather than creating direct behavioral change reveals the limitation of coercive normative instruments. The fact that target companies continue technology exports through third countries weakens the effectiveness of sanctions. As emphasized in Finnemore and Sikkink's norm life cycle model, sanctions accelerate the normative socialization process but are not sufficient alone (Finnemore & Sikkink, 1998).

General Synthesis: Strategic Recoding of Normative Power

The discussion reveals that the Union transformed digital instruments into normative power strategy during the 2010-2025 period. Market leverage, discursive legitimacy, and co-design mechanisms produce the Union's normative impact. Internal institutional coherence within the Union, third actors' market dependency, and great power competition regulate the level of normative impact. Normative power is exercised through forms of epistemic and infrastructural control, operating through technical standards and digital infrastructure beyond value transfer.

However, the effectiveness of normative power encounters structural limitations. Internal consistency deficit, legitimacy problem in the Global South, multipolar normative competition, and resistance from actors without market dependency weaken the Union's normative hegemony. The strategization of normative power creates tension between value and interest, opening new debates on the Union's foreign policy legitimacy.

In conclusion, normative power in the digital age is being recoded in the triad of institutions, infrastructure, and networks. The Union's normative power can be made sustainable through policy designs that strengthen the interaction of this triad, ensure internal consistency, and develop multi-stakeholder and inclusive norm production processes. The future of normative power depends on increasing operational effectiveness as much as defending values, and strengthening strategic foresight as much as preserving ethical foundations.

Conclusion and Recommendations

This research has examined through which mechanisms the European Union integrated digital tools into its normative power strategy during the 2010--2025 period, the dynamics of strategization that emerged in this process, and the concrete indicators of normative impact in third countries. The findings reveal that the Union's normative power has undergone a fundamental transformation in the digital age, demonstrating that value-based identity has been integrated with strategic instrumentalization and repositioned in the global order through forms of epistemic and infrastructural control.

The General Data Protection Regulation has directly influenced the data protection legislation of one hundred and fifty countries, demonstrating how the Union's normative power achieves global standardization through market leverage mechanisms (Bradford, 2020). The adoption of GDPR principles such as consent-based data processing, the right to be forgotten, data portability, and independent supervisory authorities into legislative texts by countries from different geographies such as Brazil, India, Japan, South Korea, and South Africa demonstrates that normative diffusion operates at a conceptual level (Kuner, Bygrave & Docksey, 2020; Lynskey, 2015). The Regulation's penalties exceeding one hundred and sixty million euros and the restructuring of global technology companies' entire operational structures—from product design to corporate culture—according to Union standards reveal that normative power is not merely a discursive but also a materially consequential capacity (Bradford, 2023). The 2022--2024 implementation process of the Digital Services Act and Digital Markets Act concretizes the expansion of the Union's normative impact into areas of algorithmic governance and platform economy. The designation of six platforms—Meta, Alphabet, Apple, Amazon, and ByteDance—as gatekeepers; the obligation of these platforms to disclose content algorithms, comply with data combination prohibitions, revise app store competition rules, and accept interoperability standards demonstrates that the Union's regulatory capacity is restructuring the global digital ecosystem (Keller, 2021; Cohen, 2019; Pasquale, 2015). The Commission's access to platform databases and the obligation to open data to independent researchers strengthens the epistemic dimension of normative power. This situation reveals that the Union positions its digital norms not merely as rules but as instruments controlling knowledge production and distribution processes.

In combating disinformation, the 2022 Strengthened Code of Practice bringing together thirty-four signatories—including global platforms, the advertising sector, civil society organizations, and fact-checking institutions—demonstrates how the co-design mechanism reduces normative resistance (Benkler, Faris & Roberts, 2018; Checkel, 2001). Platforms' compliance in content moderation and political advertising transparency during the 2024 European Parliament elections reveals that voluntary participation is supported by the threat of regulatory sanctions. However, the Union's limited capacity in content production in languages such as Arabic, Turkish, Persian, and Urdu weakens the global reach of digital diplomacy (Aral, 2020).

The European External Action Service's Strategic Communication Division conducting a disinformation campaign in twenty-four languages during the 2022 Ukraine crisis demonstrates that digital diplomacy supports normative power (Bjola & Holmes, 2015). The East Strategic Communication Task Force's weekly documentation of Russian-origin disinformation networks strengthens the informational dimension of normative power.

However, China's content production capacity in sixty languages and Russia's broadcasting capacity in thirty languages reveal the Union's insufficient digital diplomacy budget and the multipolar structure of global normative competition.

The design of the digital vaccination certificate application during the pandemic, preserving data minimization (sharing only certificate status), purpose limitation (use only for travel), and temporary duration (ninety-day validity) principles, demonstrates the Union's effort to maintain normative consistency even in crisis moments (Purnhagen et al., 2020: 297-306; Wendt, 1999). However, France's mandatory certificate requirement for restaurant and shopping center access, Hungary and Poland's restriction of media freedom through emergency laws during the pandemic reveals the lack of normative alignment among member states. This situation demonstrates that intra-Union internal consistency directly affects normative credibility and reduces third countries' motivation to adopt Union standards (Börzel & Risse, 2012).

The 2020 Global Human Rights Sanctions Regime's application of sanctions to companies exporting cyber surveillance technologies such as Israel's Candiru and the United Arab Emirates' Group Enso concretizes the coercive dimension of normative power (Tocci, 2008; Finnemore & Sikkink, 1998). The 2023 export restrictions applied to China's facial recognition technology producing companies demonstrate how normative power is combined with trade policy. Findings reveal that sanctions function more as normative signaling rather than creating direct behavioral change; however, technology companies avoid doing business with the Union due to reputational risk.

The Transatlantic Trade and Technology Council's strengthening of coordination in areas of data flows, artificial intelligence standards, and supply chain security demonstrates partial convergence (Keohane & Nye, 2012). The 2023 Data Privacy Framework's resolution of post-Schrems II uncertainty and stabilization of the transatlantic data economy reveals that common interests support normative convergence (Bradford, 2020; Bygrave, 2014). However, the Union's penalties of 2.4 billion euros to Alphabet, 1.2 billion euros to Meta, and 1.8 billion euros to Apple demonstrate that transatlantic tensions continue and the Union's determination to preserve normative autonomy.

In the enlargement region, Serbia and Montenegro's construction of digital harmonization roadmaps according to Union standards, enactment of GDPR-based national data protection laws, and adoption of Digital Services Act principles demonstrate that candidate countries' normative alignment is strengthened by membership perspective (Kulińska, 2020: 280-296). However, the slow progress of data protection implementation in Albania, the fragmented structure of digital regulations in Bosnia and Herzegovina, and institutional capacity insufficiency in Kosovo reveal that normative transfer cannot be limited to legal compliance alone. Digital cooperation with Turkey's dependence on customs union update and political conditions demonstrates that the effectiveness of normative power is also dependent on geopolitical factors (Tocci, 2008).

The acceptance of the Union's multi-stakeholder governance and human rights-based internet access proposals as reference documents at the United Nations Internet Governance Forum in 2021, and the Union's decisive contribution to the digital public infrastructure

agenda at the 2023 G20 summit demonstrate that normative leadership is accepted in multilateral platforms (Manners, 2002; Castells, 2009). However, Global South countries' concerns about digital divide, technology transfer, and data sovereignty; China's New International Information Order proposal; and Russia's sovereign internet model reveal the structural obstacles to multipolar digital normative competition.

The theoretical contribution of this research is its conceptualization of the strategization of normative power in the digital age. While normative power in Manners' original formulation was an identity-based and value-oriented approach (Manners, 2002), this study reveals that normative power is repositioned as a competitive capacity supported by epistemic control, infrastructural hegemony, and market leverage (Barnett & Duvall, 2005). Therefore, the concept of "strategic normative power" requires reconsideration of power theories in international relations literature and development of indicators for measuring normative power.

Recommendations for policymakers aim to strengthen the sustainability of normative power along three fundamental axes. First, the communicative dimension of normative legitimacy must be systematized. The Union should present its digital norms not as economic imposition but as ethical standards developed to protect universal rights and construct democratic digital order. Digital partnerships with African, Asian, and Latin American countries in particular can increase the inclusiveness of the Union's normative discourse and reduce digital colonialism criticisms. Second, multi-stakeholder processes in digital norm production must be institutionalized. Active participation of civil society organizations, private sector, academic institutions, and target country representatives in normative standards formation will strengthen legitimacy and reduce resistance in implementation (Checkel, 2001; Finnemore & Sikkink, 1998). Third, normative impact measurements must be operationalized. When evaluating foreign policy instruments, the Union should develop "normative impact indices" consisting of observable indicators such as terminological similarity in legislative texts, changes in platform policies, citations in multilateral documents, and civil society support levels to systematically monitor concrete outcomes of norm export.

The Union's digital diplomacy emerges as an instrument strengthening the strategic dimension of normative power. However, increasing content production in languages such as Arabic, Turkish, Persian, Swahili, Portuguese, and Urdu; developing communication strategies adapted to local contexts; and conducting interactive campaigns on digital platforms will expand the global reach of normative discourse (Bjola & Holmes, 2015; Aral, 2020). Cyber dialogue platforms, digital partnership agreements, and democratic digitalization programs enable the institutionalization of normative values through diplomatic channels. This process demonstrates the need to conceptualize and operationalize digital normative diplomacy.

The limitations of this research stem from the lack of deepened comparative perspective. Systematic comparison with actors outside the Union, particularly China's digital authoritarianism model, the United States' technological dominance approach, and Russia's disinformation networks, can more clearly reveal the Union's position. Future research should conduct in-depth analysis of the global dynamics of digital normative competition, particularly in areas of artificial intelligence governance, quantum computing standards, and cybersecurity norms. Additionally, empirical studies on how the Union's digital norms are

perceived in third countries, under which conditions they are internalized, and which local factors facilitate or hinder compliance will contribute to understanding normative effectiveness.

At the academic level, this study proposes reconceptualizing normative power as a strategic capacity form. In the digital age, norms function not merely as passive value carriers but as active instruments supported by epistemic control, infrastructural hegemony, and market leverage in shaping global order (Barnett & Duvall, 2005; Cohen, 2019; Pasquale, 2015). This situation requires reconsideration of the concept of power in international relations theory and development of indicators for measuring normative power. Future studies can enable operational-level understanding of the concept by developing normative impact indices consisting of measures such as terminological overlap rates in legislative texts, quantitative analysis of changes in platform policies, citation frequencies in multilateral documents, and civil society support levels.

In conclusion, the European Union's normative power in the digital age during the 2010--2025 period indicates a dual evolution toward both preserving value-based identity and developing strategic instruments. This process demonstrates that the Union has become not merely a norm producer but one of the geopolitical architects of digital order in the international system. Regulatory instruments such as the General Data Protection Regulation, Digital Services Act, and Digital Markets Act demonstrate that normative values are transformed into global standards through market leverage, discursive legitimacy, and co-design mechanisms (Bradford, 2020, 2023; Kuner, Bygrave & Docksey, 2020; Lynskey, 2015; Keller, 2021). However, the sustainability of this power depends on ensuring intra-Union internal consistency, strengthening perceived legitimacy in third countries, institutionalizing multi-stakeholder norm production processes, and increasing digital diplomacy capacity (Börzel & Risse, 2012; Checkel, 2001; Bjola & Holmes, 2015). The balance between normative values and strategic instruments will determine the Union's future global position. The export of digital norms must be pursued not merely for economic interests but for the purpose of protecting universal values, constructing democratic digital order, and strengthening inclusive global governance (Manners, 2002; Diez, 2005; Wendt, 1999). The Union's normative power will continue its existence as a legitimate and effective actor in global order to the extent that it can preserve this balance and maintain its distinctive position based on ethical foundations in multipolar digital competition.

References

Aral, S. (2020). *The hype machine: How social media disrupts our elections, our economy, and our health---and how we must adapt.* Currency.

Bania, K., & Geradin, D. (Eds.). (2024). *The Digital Markets Act: A guide to the regulation of Big Tech in the EU*. Hart Publishing.

Barnett, M., & Duvall, R. (Eds.). (2005). *Power in global governance.* Cambridge University Press.

Barrett, G., Müller-Graff, P.-C., Rageade, J.-P., & Vadász, V. (Eds.). (2024). *European sovereignty: The legal dimension.* Springer.

Beaucillon, C. (Ed.). (2024). *EU sanctions law and policy: Thematic and country regimes in practice*. Edward Elgar.

Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics.* Oxford University Press.

Bickerton, C. J. (2012). *European integration: From nation-states to member states.* Oxford University Press.

Bigo, D., Isin, E., & Ruppert, E. (Eds.). (2019). *Data politics: Worlds, subjects, rights.* Routledge.

Birnhack, M. D., & Mundlak, G. (2025). The Brussels effect(s) and the rise of a privacy profession. *International Data Privacy Law*, *ipaf005*, 1--19.

Biscop, S. (2019). *European strategy in the 21st century: New future for old power.* Routledge.

Bjola, C., & Holmes, M. (2015). *Digital diplomacy: Theory and practice.* Routledge.

Bjola, C., & Manor, I. (Eds.). (2024). *The Oxford handbook of digital diplomacy*. Oxford University Press.

Börzel, T. A., & Risse, T. (2012). From Europeanisation to diffusion: Introduction. *West European Politics, 35*(1), 1-19.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology.* Oxford University Press.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world.* Oxford University Press.

Braun, V., & Clarke, V. (2022). *Thematic analysis: A practical guide.* SAGE.

Bretherton, C., & Vogler, J. (2013). *The European Union as a global actor* (3rd ed.). Routledge.

Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics.* Harvard University Press.

Bygrave, L. A. (2014). *Data privacy law: An international perspective.* Oxford University Press.

Calo, R., Pasquale, F., & Zarsky, T. (Eds.). (2018). *The Cambridge handbook of consumer privacy.* Cambridge University Press.

Carrapico, H., & Farrand, B. (2025). EU Data Sovereignty: An Autonomy-Interdependence Governance Gap? *Politics and Governance, 13,* 1-16.

Castells, M. (2009). *Communication power.* Oxford University Press.

Chaban, N., & Elgström, O. (2024). European Union Normative Positions, Resilience and Contestation: A Perceptual Approach. *JCMS: Journal of Common Market Studies,* 1-18.

Chadwick, A. (2017). *The hybrid media system: Politics and power* (2nd ed.). Oxford University Press.

Chalmers, D., Davies, G., & Monti, G. (2019). *European Union law* (4th ed.). Cambridge University Press.

Chander, A., & Sun, H. (Eds.). (2023). *Data sovereignty: From the Digital Silk Road to the return of the state.* Oxford University Press.

Checkel, J. T. (2001). Why comply? Social learning and European identity change. *International Organization, 55*(3), 553-588.

Clavé, P. (Ed.). (2024). *Global digital data governance: Polycentric perspectives*. Routledge.

Cohen, J. E. (2019). *Between truth and power: The legal constructions of informational capitalism.* Oxford University Press.

Costello, R. Á., & Leiser, M. (Eds.). (2024). *Critical reflections on the EU's data protection regime: GDPR in the machine*. Hart Publishing.

Couldry, N., & Mejias, U. A. (2019). *The costs of connection: How data is colonizing human life and appropriating it for capitalism*. Stanford University Press.

Craig, P., & de Búrca, G. (2020). *EU law: Text, cases, and materials* (7th ed.). Oxford University Press.

Crawford, K. (2021). *Atlas of AI: Power, politics, and the planetary costs of artificial intelligence.* Yale University Press.

Daniels, C., Erforth, B., & Teevan, C. (Eds.). (2022). *Africa--Europe cooperation and digital transformation*. Routledge.

DeNardis, L. (2014). *The global war for internet governance.* Yale University Press.

DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch.* Yale University Press.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2023). *The SAGE handbook of qualitative research* (6th ed.). SAGE.

Diez, T. (2005). Constructing the self and changing others: Reconsidering 'normative power Europe'. *Millennium: Journal of International Studies, 33*(3), 613-636.

Džankić, J., Keil, S., & Kmezić, M. (Eds.). (2019). *The Europeanisation of the Western Balkans: A failure of EU conditionality?* Palgrave Macmillan.

Eeckhout, P. (2011). *EU external relations law* (2nd ed.). Oxford University Press.

Egan, M., Raube, K., Wouters, J., & Chaisse, J. (Eds.). (2023). *Contestation and polarization in global governance.* Edward Elgar.

Elliffe, C. (2021). *Taxing the digital economy: Theory, policy and practice*. Cambridge University Press.

Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR) relevant theory? *International Political Science Review*, *27*(3), 221--244.

Eskhita, R., & Stamhuis, E. (2024). The Influence of the Brussels Effect on the Interpretation of Data Protection Laws in the Gulf. *Global Journal of Comparative Law, 13*(2), 261-278.

Farrell, H., & Newman, A. L. (2019). *Of privacy and power: The transatlantic struggle over freedom and security*. Princeton University Press.

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization, 52*(4), 887-917.

Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality.* Oxford University Press.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People---An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and machines*, *28*(4), 689-707.

Frey, C. B. (2019). *The technology trap: Capital, labor, and power in the age of automation.* Princeton University Press.

Garton Ash, T. (2016). *Free speech: Ten principles for a connected world.* Yale University Press.

Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media.* Yale University Press.

Gorwa, R. (2024). *The politics of platform regulation: How governments shape online content moderation*. Oxford University Press.

Greer, S. L., King, E., & Jarman, H. (2025). *Pandemic polity-building: Europe's digital emergency*. Oxford University Press.

Gstöhl, S., & Schunz, S. (Eds.). (2021). *The external action of the European Union: Concepts, approaches, theories* (2nd ed.). Red Globe Press.

Helberg, J. (2021). *The wires of war: Technology and the global struggle for power*. Simon & Schuster.

Helbing, D. (2015). *Thinking ahead: Essays on big data, digital revolution, and participatory market society.* Springer.

Hill, C., Smith, M., & Vanhoonacker, S. (Eds.). (2017). *International relations and the European Union* (3rd ed.). Oxford University Press.

Hilty, L. M., & Bieser, J. (2017). *Opportunities and risks of digitalization for climate protection in Switzerland*. University of Zurich, Informatics and Sustainability Research Group.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2017). *Digital citizenship in a datafied society.* Polity.

Hix, S., & Høyland, B. (2022). *The political system of the European Union* (4th ed.). Red Globe Press.

Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives.* Yale University Press.

Howorth, J. (2014). *Security and defence policy in the European Union* (2nd ed.). Palgrave Macmillan.

Husovec, M. (2024). *Principles of the Digital Services Act*. Oxford University Press.

Jørgensen, K. E., Aarstad, A. K., Drieskens, E., Laatikainen, K., & Tonra, B. (Eds.). (2015). *The SAGE handbook of European foreign policy.* SAGE Publications.

Kaldor, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Polity.

Karathanasis, T. (2025). *Cybersecurity and EU law: Adopting the Network and Information Security Directive.* Routledge.

Karjalainen, T. (2023). European norms trap? EU connectivity policies and the case of the global gateway. *East Asia, 40*(3), 293-316.

Kaye, D. (2019). *Speech police: The global struggle to govern the internet.* Columbia Global Reports.

Keller, D. (2021, May). *US developments and the DSA* [Presentation slides]. In European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies (Ed.), *The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective* (Workshop, IMCO Committee).

Kello, L. (2017). *The virtual weapon and international order.* Yale University Press.

Keohane, R. O., & Nye, J. S. (2001). *Power and interdependence* (3rd ed.). Longman.

Keohane, R. O., & Nye, J. S. (2012). *Power and interdependence* (4th ed.). Pearson.

Keukeleire, S., & Delreux, T. (2022). *The foreign policy of the European Union* (3rd ed.). Bloomsbury Academic.

Klimburg, A. (2017). *The darkening web: The war for cyberspace.* Penguin Press.

Kosseff, J. (2019). *The twenty-six words that created the Internet*. Cornell University Press.

Koutrakos, P. (2015). *EU international relations law* (2nd ed.). Hart Publishing.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy.* Princeton University Press.

Krotoszynski, R. J., Jr., Koltay, A., & Garden, C. (Eds.). (2025). *Disinformation, misinformation, and democracy: Legal approaches in comparative context*. Cambridge University Press.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary.* Oxford University Press.

Laidlaw, E. B. (2015). *Regulating speech in cyberspace: Gatekeepers, human rights and corporate responsibility.* Cambridge University Press.

Laïdi, Z. (Ed.). (2008). *EU foreign policy in a globalized world: Normative power and social preferences.* Routledge.

Kulińska, M. (2020). Cross-Border Commercial Disputes: Jurisdiction, Recognition and Enforcement of Judgments After Brexit. *Croatian Yearbook of European Law & Policy*, *16*(1), 279-300.

Lavenex, S., & Schimmelfennig, F. (2013). EU rules beyond EU borders: theorizing external governance in European politics. In *EU External Governance* (pp. 791-812). Routledge.

Lessig, L. (2006). *Code: And other laws of cyberspace (version 2.0).* Basic Books.

Liebetrau, T. (2024). Problematising EU cybersecurity: Exploring How the single market functions as a security practice. *JCMS: Journal of Common Market Studies, 62*(3), 705-724.

Lucarelli, S., & Manners, I. (Eds.). (2006). *Values and principles in European Union foreign policy.* Routledge.

Lynskey, O. (2015). *The foundations of EU data protection law.* Oxford University Press.

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies, 40*(2), 235-258. https://doi.org/10.1111/1468-5965.00353

Manners, I. (2008). The normative ethics of the European Union. *International Affairs, 84*(1), 45-60.

Mansell, R., & Raboy, M. (Eds.). (2011). *The handbook of global media and communication policy.* Wiley-Blackwell.

Marsden, C. T. (2011). *Net neutrality: Towards a co-regulatory solution.* Bloomsbury Academic.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Morozov, E. (2011). *The net delusion: The dark side of internet freedom.* PublicAffairs.

Mortensen, M., & Pantti, M. (Eds.). (2023). *Media and the War in Ukraine* (Global Crises and the Media, Vol. 29). Peter Lang.

Mueller, M. (2010). *Networks and states: The global politics of internet governance.* MIT Press.

Napoli, P. M. (2019). *Social media and the public interest: Media regulation in the disinformation age.* Columbia University Press.

Nye, J. S. (2004). *Soft power: The means to success in world politics.* Public Affairs.

Nye, J. S. (2011). *The future of power.* PublicAffairs.

O'Connor, C., & Weatherall, J. O. (2019). *The misinformation age: How false beliefs spread.* Yale University Press.

Pace, M. (2024). The Construction of EU Normative Power and the Middle East 'Conflict'... 16 Years on. *JCMS: Journal of Common Market Studies, 62*(3), 868-884.

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* Harvard University Press.

Pasquale, F. (2020). *New laws of robotics: Defending human expertise in the age of AI.* Harvard University Press.

Peers, S. (2016). *EU justice and home affairs law* (4th ed.). Oxford University Press.

Persily, N., & Tucker, J. A. (Eds.). (2020). *Social media and democracy: The state of the field, prospects for reform.* Cambridge University Press.

Pistor, K. (Ed.). (2020). *Law in the time of COVID-19*. Columbia Law School.

Podszun, R. (Ed.). (2024). *Digital Markets Act: Article-by-Article Commentary.* Nomos; C. H. Beck; Hart Publishing.

Pohle, J., & Thiel, T. (Eds.). (2020). *Digital sovereignty: Rethinking key concepts of a digital Europe.* Transcript Verlag.

Pomerantsev, P. (2019). *This is not propaganda: Adventures in the war against reality.* PublicAffairs.

Portela, C. (2010). *European Union sanctions and foreign policy: When and why do they work?* Routledge.

Powers, S., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom.* University of Illinois Press.

Purnhagen, K. P., De Ruijter, A., Flear, M. L., Hervey, T. K., & Herwig, A. (2020). More competences than you knew? The web of health competence for European Union action in response to the COVID-19 outbreak. *European Journal of Risk Regulation*, *11*(2), 297-306.

Ragnedda, M., & Gladkova, A. (Eds.). (2020). *Digital inequalities in the Global South.* Palgrave Macmillan.

Reinfeld, Y. (2024). *The European Union as a normative power: The role of the CJEU.* Routledge. https://doi.org/10.4324/9781003370512

Reinfeld, Y., & Gaon, A. (2025). *The European Union and Digital Law: Normative Power in a Globalized Technological Landscape.* Routledge.

Rid, T. (2020). *Active measures: The secret history of disinformation and political warfare.* Farrar, Straus and Giroux.

Risse, T. (Ed.). (2011). *Governance without a state? Policies and politics in areas of limited statehood.* Columbia University Press.

Roberts, S. T. (2019). *Behind the screen: Content moderation in the shadows of social media.* Yale University Press.

Russell, S., & Norvig, P. (2021). *Artificial intelligence: A modern approach* (4th ed.). Pearson.

Saurugger, S., & Terpan, F. (2017). *The Court of Justice of the European Union and the politics of law.* Palgrave Macmillan.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* W. W. Norton & Company.

Scholten, M. (Ed.). (2023). *Research handbook on the enforcement of EU law*. Edward Elgar.

Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed.* Yale University Press.

Singer, P. W., & Brooking, E. T. (2018). *LikeWar: The weaponization of social media.* Houghton Mifflin Harcourt.

Sjursen, H. (2006). The EU as a 'normative' power: How can this be? *Journal of European Public Policy, 13*(2), 235-251. https://doi.org/10.1080/13501760500451600

Smith, B., & Browne, C. (2019). *Tools and weapons: The promise and the peril of the digital age.* Penguin Press.

Solove, D. J., & Schwartz, P. M. (2021). *Information privacy law* (7th ed.). Aspen Publishing.

Srnicek, N. (2017). *Platform capitalism.* Polity Press.

Stengel, R. (2019). *Information wars: How we lost the global battle against disinformation and what we can do about it.* Atlantic Monthly Press.

Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy.* Cambridge University Press.

Susskind, J. (2018). *Future politics: Living together in a world transformed by tech.* Oxford University Press.

Susskind, J. (2022). *The digital republic: On freedom and democracy in the 21st century.* Pegasus Books.

Tambini, D. (2021). *Media freedom.* Polity Press.

Tikk, E., & Kerttunen, M. (2018, October 23). *Parabasis: Cyber-diplomacy in stalemate*. Norwegian Institute of International Affairs (NUPI).

Tocci, N. (2007). *The EU and conflict resolution: Promoting peace in the backyard.* Routledge.

Tocci, N. (2007). Profiling Normative Foreign Policy: The European Union and Its Global Partners. *CEPS Working Document No. 279.* Centre for European Policy Studies. https://ssrn.com/abstract=1337974

Tocci, N. (2008). *The European Union as a normative foreign policy actor* (CEPS Working Document No. 281). Centre for European Policy Studies.

Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest.* Yale University Press.

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world.* Oxford University Press.

Veale, M., & Borgesius, F. Z. (2021). Demystifying the draft EU artificial intelligence act. *arXiv preprint arXiv:2107.03721*, 97-112.

Véliz, C. (2020). *Privacy is power: Why and how you should take back control of your data.* Melville House.

Voigt, P. (2025). *The EU AI Act: Answers to frequently asked questions*. Springer.

Wendt, A. (1999). *Social theory of international politics.* Cambridge University Press.

Whyte, C. (2020). Beyond tit-for-tat in cyberspace: Political warfare and lateral sources of escalation online. *European Journal of International Security*, *5*(2), 195--214.

Yakovleva, S., & Irion, K. (2020). Pitching trade against privacy: Reconciling EU governance of personal data flows with external trade. *International Data Privacy Law, 10*(3), 201-221. https://doi.org/10.1093/idpl/ipaa003

Yilma, K. (2023). *Privacy and the role of international law in the digital age.* Oxford University Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power.* PublicAffairs.