Beyond borders:

Trust Mechanisms Shaping EU Digital Governance

Student Name: Irene Bi

Student No. 300325609

Supervised by: Professor Alexandra Gheciu

Abstract

In the digital age, digital technology and its associated challenges have brought digital governance into the global spotlight. The European Union (EU) has risen to the occasion, transcending national borders to foster cooperation in digital governance and establish significant mutual trust. This paper adopts a liberal institutionalist perspective to analyze the development, institutions, and cooperation of EU digital governance, focusing on institutional trust. Under institutional trust, it mainly examines two models: compulsory and favorable trust mechanisms, influenced by market economy and regional security factors. Furthermore, building upon the relatively robust institutional trust, this paper also suggests an enhanced solidarity-based trust mechanism founded on the shared values and identity of the EU, aimed at further solidifying institutional trust in the framework of liberal institutionalism. Although the evidence of solidarity-based trust mechanism already exists in the EU, it needs to be improved by continuous construction. Finally, this paper uses the practical application of the General Data Protection Regulation (hereinafter referred to "GDPR") during the Covid-19 pandemic as an example of how the EU's trust mechanisms for digital governance remain effective and robust even during a global crisis.

Key words: trust mechanisms, European Union, digital governance, GDPR

CONTENTS

Introduction

With the deepening of the globalization process, scholars have shown an increased interest in researching global governance. Generally, there is a consensus on the following trends in global governance. Firstly, global governance issues have expanded beyond national security and international trade to include a diverse array of fields, such as climate change, energy crisis, digital transformation, etc. Secondly, there has been a shift in the main players involved in global governance, moving away from traditional actors like states and intergovernmental organizations to a diverse range of stakeholders, including associations, non-governmental organizations, and decentralized communities.[1] Finally, global governance regimes have evolved from formal rules through inter-government negotiations to include different policy tools, such as public-private partnerships, self-regulation, and experimentalist governance, giving rise to a complex network of regimes across different fields.[2]

Since the end of Cold War, digital globalization has swept the international community, bringing both opportunities and unprecedented challenges. Hotly debated issues like data theft, privacy leakage, and digital intrusion have surfaced (listed in Table 1), resulting in the weaponization of data and technology across borders. This can be understood from both economic and security perspectives. On one hand, control over digital technology means the control of global production. In the past, the strength of a country's production derives from its capacity to effectively integrate productive resources to generate wealth. In the digital era, this capability is no longer contingent on geographic or demographic factors. This shift occurs

[1] Nye, Joseph S. *The Regime Complex for Managing Global Cyber Activities.* CIGI, 2014, p.5.
[2] Raustiala, Kal, and David G. Victor. "The Regime Complex for Plant Genetic Resources." *International Organization*, vol. 58, no. 2, 2004, pp. 277–309.

because data and technology are replacing traditional human roles, and wealth generation is not tied to specific territories in the same manner as with physical resources.[3] On the other hand, with the growth of battle for information resources, this fact raises questions about cybersecurity, and cyberwar. Digital espionage and remote access to critical infrastructure are also increasing national security concerns. Individual states face significant challenges due to the remote and often international origins of the perpetrators, which can be far beyond their borders. We are now witnessing the digital transformation of power, where the advantages of digital development will be pivotal in national strategic competition.[4] State competition now transcends traditional geopolitical constraints, with state power no longer confined solely by demographic and geographic limitations. The possession of data stands as the foremost asset in the digital world, serving as a key source of political power and a means of safeguarding national security. Therefore, digital technology transcends geographic borders, making digital governance issues inherently global rather than domestic.[5] Global cooperation is needed to mitigate national governance disputes at the political level by realizing unification or interoperability on the institutional level. It seeks to synchronize the actions of diverse stakeholders to effectively manage the governance risks associated with digital transformation across domains.[6] These imperatives give rise to what we term "global digital governance" in this paper.

[3] The Economist. "How technology is redrawing the boundaries of the firm", 2023. https://www.economist.com/business/2023/01/08/how-technology-is-redrawing-the-boundaries-of-the-firm. Accessed: March 1, 2024.
[4] Dear, Keith. "Beyond the 'Geo' in Geopolitics: The Digital Transformation of Power." *The RUSI Journal*, vol. 166, no. 6–7, 2021, pp. 20–31.
[5] Voronkova, V., Punchenko, O., & Azhazha, M. "Globalization and global governance in the fourth industrial revolution (industry 4.0)". *Humanities Studies*, 2020, p.182.
[6] Jia, Kai, and Shaowei Chen. "Global Digital Governance: Paradigm Shift and an Analytical Framework." *Global Public Policy and Governanc*e, vol. 2, no. 3, 2022, p.286.

Table 1: Research topics of global digital governance[7]

Topic areas	Technical types	The main problem	Representative literature
Global governance of digital technology	Internet	Global management of Internet Protocol standards	Tassey et al. 2009; Claessen, 2020
	Artificial intelligence	Externality, ethics, subjectivity, and other risks	Sweeney, 2013; Acemoglu & Restrepo, 2020;
	Blockchain	Law lag and malicious use risk	Goldfeder et al. 2018; Zīle & Strazdiņa, 2018
	Algorithm	Rule "black box" and discriminatory risk	Edwards & Veale, 2018; Huq 2019
	Robotics and Automation systems	Decision-making "black box", responsibility risk	Noorman & Johnson, 2014; O'Sullivan et al. 2019
	Quantum computing	Data security risk	Fedorov et al. 2018; Molina et al. 2021
	Internet of things	Data security risk	Xi & Ling 2016; Kim 2017
	Digital Finance Technology	Privacy risk and system vulnerability risk	Zetzsche et al. 2020; Ozili 2020
Global governance of the digital industry	Digital currency	Legal lag and anti-money laundering risk	Cumming et al. 2019; Whitford & Anderson, 2020
	Cross-border data flow	Consistency of data rights protection rules	Kong, 2010; Aaronson 2019
	Digital tax	Rational distribution of tax base and tax avoidance risk	Corkery et al. 2013; Peng 2016
	Digital platform	Platform power risk	Cutolo & Kenney 2021
	Sharing economy	Distribution and labor protection	Schor & Attwood-Charles 2017; Wu & Li 2019
	E-commerce	Intellectual property protection	Zhou 2021
	Online false information	Public opinion governance and ideology management	Clayton et al. 2020; Molina et al. 2021

In times of heightened uncertainty and global transition, trust gradually emerges as a scarce and critical asset. Since digital information is closely related to national economic and security interests, each country exhibits its own preferences and priorities in digital-related governance. While some countries are still seeking assistance and struggling to develop their digital infrastructure, others have already established relatively robust and comprehensive institutional rules for digital governance systems. This trend has contributed to variations in digital governance norms among nations, leading to the fragmentation of global digital governance standards. Therefore, in the sphere of digital governance, digital trust becomes a new concept that has emerged with the widespread adoption of new-generation information technologies.

In this context, due to EU's high level of integration, scholars have chosen it as a representative for digital governance research. A definition of European governance is given by the European Commission in the White Paper: "Governance means rules, processes and behavior that affect the way in which powers are exercised at European level, particularly as regards openness, participation, accountability, effectiveness and coherence"[8] This definition emphasizes the principles guiding the EU's interactions with other decision-making actors,

[7] Jia, Kai, and Shaowei Chen, p.287.
[8] European Commission, European Governance: A White Paper, *Brussels*, 2001, COM (2001) 428 p.3.

whether public or private. In terms of EU digital governance, the effort has been approached more from an intergovernmental point of view (Peterson and Bomberg 1999). The EU now has developed mature institutions for digital governance along with numerous relevant initiatives in the field. It has effectively overcome certain the sovereignty barriers among Member States in the digital governance through well-established institutions, thus establishing a robust institutional trust relationship, serving as a valuable model for international cooperation. Considering the role played by EU institutions in governance and the necessity of these institutions for EU Member States, the objective of this paper is to embrace the liberal institutionalist perspective in order to answer the following questions: What are the strengths of the EU's digital governance institutions? How to develop effective institutional trust among EU Member States? Where is EU digital governance cooperation headed in the future?

The integration of EU digital governance and the theory of trust is a valuable approach to understanding the dynamics of effective cooperation at the supranational level. Despite the anarchic nature of the international community, it is still possible to establish trustworthy institutions in global digital governance. Analyzing the motives, modes, and influencing factors of EU Member States' trust mechanisms towards EU institutions related to digital governance can offer valuable insights for the establishment of international institutions for global digital governance at the international level across various countries. This research contributes to the broader understanding of trust dynamics in the context of digital governance and provides a reference for international collaboration in this crucial field.

Chapter I: Definition of Trust Mechanisms

The term "trust" was originally a psychological concept, perceived as a psychological state driven by the desire to secure the cooperation of the trustee in order to attain valued results or resources.[9] In the 20th century, trust mechanisms expanded into sociology and political science, becoming an interdisciplinary concept. Today, the convergence of digital governance and trust mechanisms provides a new perspective on international cooperation.

1. Trust Mechanisms in Sociology

In the early 20th century, Simmel, a pioneer in contemporary sociology's study of trust, asserts that "trust is one of the most important synthetic forces within society".[10] Trust then becomes a specialized topic in sociology in the 1970s, with scholars like the Polish sociologist Piotr Sztompka building upon earlier studies. Sztompka emphasized not only interpersonal trust but also the significance of trust in the functioning of the entire social system.

From an individualistic perspective, Sztompka defines trust as a bet of the future contingent actions of others.[11] This definition suggests that trust consists of two main components: belief and commitment, and meanwhile emphasizing the uncertainty and risk in interpersonal interactions. It is to behave as though the future were certain.[12] Trust emerges as a spontaneous need and emotion within the dynamics of social interaction, representing social relationships. As societies transition from traditional to modern forms, interpersonal trust extends to trust in the entire social system, shifting from passive to active modes.

---

[9] Simpson, J. A. (2007). *Psychological Foundations of Trust. Current Directions in Psychological Science*, 16(5), p. 264−268.
[10] Simmel, G. 1950. *The Sociology of Georg Simmel. Transi*., ed. and intr. by K. H. Wolff. New York: Free Press, p.318.
[11] Sztompka, Piotr. *Trust: A Sociological Theory.* Cambridge University Press, 1999, p.25.
[12] Luhmann, Niklas, et al. *Trust and Power*. Wiley, 1979, p.10.

From the perspective of the social system, trust is considered as the prerequisite for social order, and it is also considered as a product of a social order of a particular type.[13] In particular, Sztompka highlights the relationship between democracy and culture of trust, suggesting that, all else being equal, trust is more likely to appear in a democracy than in any other type of political system. This is because democracy has the capacity to institutionalize the distrust inherent in the system. In a democratic setup governed by the rule of law, the distribution of power is limited through mutual checks and balances among different institutions and government branches. Sztompka's insight informs the paper's exploration of trust mechanisms within the EU context. In a democratic system, the EU offers Member States a robust framework of accountability grounded in the principle of the system's legitimacy, reinforced by binding and stable constitutions, leading to institutional trust.

Since then, the study of trust in sociology is getting richer, and the concept of trust begins to take on a political science dimension.

2. Trust Mechanisms in Political Science

The modernization has integrated trust into the realm of political science, reflecting shifts in the government-citizen and state-society relationship. This evolution expands the study of trust mechanisms to include three dimensions: individuals, society, and government.

Actually, there are many alternative concepts for the term "trust" in political science, including "trust in political institutions" and "confidence in government". It is difficult to differentiate between the two as they exhibit a strong correlation and similarity. Nevertheless, the theoretical framework of political trust, as developed by political scientists such as David

[13] Sztompka, Piotr. *Trust: A Sociological Theory.* Cambridge University Press, 1999, p.139.

Easton and Pippa Norris, delineates from generalized support by defining political trust as confined to a specific set of objects, while also emphasizing psychological factors. In this framework, the objects include, on one hand, the core institutions of liberal democracy—including parliament, government, the justice system, as well as the civil service, the police, and the military—and, on the other hand, incumbent political officeholders such as party leaders, legislators, and public officials.[14] Thus, political trust is characterized as both relational and situational, as it involves a subject who trusts and an object that is trusted.

In addition, it reflects orientations towards the nation-state, its agencies, and actors. When citizens hold positive orientations, they acknowledge the legitimacy of states to govern within territorial boundaries. They do not question the fundamental constitutional structure and rules, nor the authority of officeholders. Therefore, the most fundamental attitudes of citizens towards belonging to the nation-state are exemplified by feelings of national pride, patriotism, and identity. Citizens also hold agreement with core principles and normative values upon which the regime is based, including approval of democratic values and ideals.[15] "Trust" here is perceived as a psychological orientation and concerned about the role of values and identity.

This trust framework highlights the significance of identity and values in trust formation, paving the way for potential deeper cooperation among EU Member States in the future.

3. Trust Mechanisms in Digital Governance

As mentioned above, trust is relational, manifesting in both personal and impersonal forms. In contrast, within the context of global governance, trust relations are primarily examined

[14] Zmerli, Sonja, and Tom W. G. van der Meer. "The Deeply Rooted Concern with Political Trust." *Handbook on Political Trust*, Edward Elgar Publishing, 2017, p.4.
[15] *Ibid.*, p.87.

between states and institutions at the international level. Morton Deutsch is the first scholar to introduce the concept of trust into the study of international relations. Trust involves a belief or expectation that a certain outcome will occur, and entities act based on this belief. The impact of such actions can be positive when they align with expectations, fostering a sense of reliability and confidence.[16] Trust, in this context, is the expectation of a state regarding the behavior of other states to maximize its own interests. Since then, trust theory has been applied to the study of state cooperation and non-cooperation.

In this paper, trust is discussed in the conceptual framework of liberal institutionalism, taking the form of institutional trust. Institutional trust is primarily limited to impersonal relationships with and between institutions, including international organizations, regimes, and conventions. Trusting an institution means that someone will follow the institutions' directions, because doing so is in his own best interest.[17] At the same time, institutions recognize that maintaining trust is essential to secure compliance and justify the rules. This fact limits and binds the actions of institutions in question to the vulnerability of the trustor. In this way, trust puts an obligation on institutions via the normative expectation that it will act in the interest of those trusting it. Institutional trust signals an engagement in cooperative behavior with or between institutions, and the justifiable acceptance of a form of authority despite uncertainty surrounding future action.[18] Therefore, unlike interpersonal trust, institutional trust reflects the formalized and proceduralized nature of the relationship, ensuring trust in the institution from its constituents.

---

[16] Deutsch, Morton. "Trust and Suspicion", *The Journal of Conflict Resolution*, Vol.2, No.4, 1958.
[17] Tom R. Tyler, "Trust and Democratic Governance", *Trust and Governance*, 1998, p.280.
[18] Partiti, Enrico. "TRUST AND GLOBAL GOVERNANCE: ENSURING TRUSTWORTHINESS OF TRANSNATIONAL PRIVATE REGULATORS." *New York University Journal of International Law & Politics*, vol. 52, no. 2, 2020, p.443.

In the context of the paper's discussion on EU digital governance, the trustors are the EU Member States, while the trustees are the supernational institutions of the EU, including EU institutions, the EU bodies, decentralized agencies as well as extended regulations and rules. The trust between them is directly linked to the effectiveness of EU digital governance and the level of cooperation between Member States. Furthermore, based on the institutional trust, this paper argues that there is still room for further development of the institutional trust. Solidarity-based trust mechanism emphasizes a return to prioritizing the public interest and collective rights of the individuals involved, rather than solely focusing on the coercive nature of institutions and safeguarding the interests of the states through institutions. Although it is far from a dominant form of trust mechanism, enhancing shared value and solidarity in the future could further bolster cooperation between EU Member States.

Digital technology has opened up boundless possibilities for the advancement of the international community. However, the technology underpinning this development, along with related elements like the international institutions, the states, and organizations, has, to some extent, heightened the complexity of the trust environment. Therefore, the establishment of trust mechanisms should be incorporated into the realm of digital governance.

Chapter II: Evolution and Objectives of EU Digital Governance

As an international organization for political and economic integration, The EU originated in the 1950s. With the evolution of digital technology and the escalation of the associated digital security issues, the EU has played a vital role in ushering in the era of digital governance.

1. Evolution of EU Digital Governance

As digital technology utilization expanded, challenges of digitalization startes to surface. The EU's primary focus in digital governance revolves around data security protection during this process. The 2001 Convention on Cybercrime, signed by 26 EU Member States and 30 other nations (including the United States, Canada, Japan, and South Africa), outlines measures to combat cybercrime, including computer intrusion and electronic payment fraud, etc.[19] The Convention is the world's first international treaty specifically addressing cybercrime, emphasizing the importance of international cooperation.

From 2010, with the growing importance of personal data in the digital economy, the EU has intensified its focus on safeguarding data protection and privacy rights. At this stage, the EU has strengthened the protection of personal data and the right to privacy by implementing the GDPR. This historic legislation sets stringent standards for data processing and cross-border data flows, elevating the EU's commitment to user privacy. Under the GDPR, processing personal data requires a lawful basis, transparent delineation of processing purposes, and the collection and use of only necessary personal data. Up to this point, the EU has taken a proactive approach in advancing digital governance.

[19] Council of Europe, "Convention on Cybercrime", ETS 185-Cybercrime (Convention), 2001, https://rm.coe.int/1680081561, Accessed: 5 March 2024.

With the U.S. taking the lead in digital technology and markets, The EU is concerned about losing its competitive advantage in digital development. In 2020, the European Commission published "Shaping Europe's Digital Future", officially formalizing the EU's concept of digital sovereignty. [20] The EU begins seeking the power to control its own digital destiny, including the data, hardware, and software that it relies on and creates. Consequently, there has been a rise in EU efforts to safeguard digital sovereignty. For example, the Digital Marketplace Act exemplifies strict regulations imposed on companies with substantial influence in the digital market, coupled with antitrust investigations targeting tech giants.

To protect digital sovereignty and cybersecurity, the EU has strengthened its collaboration and defense capabilities among Member States. The EU has implemented NIS Directive and the Cybersecurity Act, mandating Member States to reinforce the security of their network infrastructures and enhance their capacity to respond effectively to cyberattacks and data breaches. However, while EU Member States manage cybersecurity at the national level, they inadvertently create vulnerabilities in international digital networks due to challenges such as regulatory fragmentation, ineffective information sharing, and cross-border coordination. To address this, the EU continually improves legislation, tightens regulations for critical infrastructures, and technical gaps. The updated NIS2 Directive in 2023 calls for the establishment of cybersecurity institutions and improved response capabilities and encourages the inclusion of new focus areas such as supply chain, vulnerability management and core Internet. [21] Furthermore, there is an increasing trend towards strict regulation of the mass

[20] Kaloudis, Martin. "Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan?" *New Global Studies,* vol. 16, no. 3, 2022, p.275, https://doi.org/10.1515/ngs-2021-0015.
[21] European Commission. "Shaping Europe's Digital Future." *Digital Strategy*, 14 Sep 2023, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

dissemination of information on the Internet to enhance cybersecurity. In 2020, the Digital Services Bill was introduced with the objective of enhancing the authenticity of information on online platforms and addressing the proliferation of fake news and illegal content. In the coming years, the EU is prioritizing the development of trustworthy AI, aiming to sustain its leadership in digital technology. Simultaneously, the focus is on ensuring that the people derive benefits from AI while upholding the core values of the EU as a collective entity.

In summary, the EU is transitioning from a traditional model of "passive governance" characterized by the development of technology preceding governance, to an era of "active governance". This approach involves anticipating digital technology trends, implementing pre-emptive management strategies, and establishing a robust security defense line.

2. Objectives of EU Digital Governance

Digital governance involves a multi-stakeholder dialogue and decision-making process for the development of shared principles and rules shaping the evolution and use of the Internet. Within the EU, the most crucial aspects of digital governance include safeguarding online security and protecting human rights in the digital era.

Maintaining cybersecurity demands significant effort as it touches on various deep-rooted issues. This includes taking action against violent extremism and radicalization, cybercrime, as well as the exploitation, harassment, and bullying of individuals online. Additionally, efforts are also needed to protect users from sexual abuse and cyber-exploitation, combat trafficking in organs and human beings, and prevent the sale of counterfeit and fake medicines.[22] In this

[22] Council of Europe, "Strategy 2016-2019, Democracy, human rights and the rule of law in the digital world", 2016, https://rm.coe.int/16806aafa9, Accessed: 6 March 2024.

context, the EU aims to promote the accession by a maximum number of countries worldwide to the Budapest Convention and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108). A comprehensive strategy is also necessary to counter violent extremism and radicalization on the Internet, involving all levels of government. Furthermore, women and children are particularly vulnerable in the digital environment, making it essential to monitor online abuse such as cyber-stalking, sexism, and threats of sexual violence.

Another key objective of EU digital governance is to respect and protect the human rights in the digital world. The Internet is an invaluable space for the exercise of fundamental rights such as freedom of expression and information. However, as connectivity to the Internet and information and communication technologies (ICTs) becomes more pervasive, there are escalating risks to the human rights of Internet users. The right to privacy is part of the 1950 European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[23] Digital tracking and surveillance, along with the collection of personal data, including sensitive health-related data, for profiling purposes, pose significant threats to privacy and the overall enjoyment of human rights. From this basis, the EU has pursued legislative measures to prevent online platforms from monopolizing users' private information and to restore trust in digital technology. The EU believes that the digital governance must be protected from political interference, and that fundamental principles such as human rights, freedom of expression, and privacy must be

[23] European Court of Human Rights. "Guide on Article 8 of the European Convention on Human Rights." Publisher or Website, 31 August 2022, https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life.

respected.[24] It is crucial that national and international legislation and government practices concerning the internet adhere to international law and are designed not only to protect but also to promote and fulfill human rights.

The EU is committed to further strengthening European dialogue and the exchange of best practices on the creation, access, and management of digital culture. This is aimed at promoting an inclusive, human-centric, rights-oriented, and environmentally sustainable vision of digital transformation.

[24] Peggy Vissers, "Global Digital Compact: Deep Dive on Internet Governance", *UN New York*, 2023.

Chapter III: Construction of Institutional Trust in the EU Digital Governance

This chapter will introduce supranational institutions associated with EU initiatives aimed at assisting Member States in establishing effective trust mechanisms within digital governance. It will explore the roles of these institutions and the challenges they encounter in the governance landscape.

1. Dynamics

EU supranational institutions play a crucial role in shaping policies and regulations and constructing institutional trust for EU digital governance. These institutions, categorized into EU institutions, bodies, and decentralized agencies, collectively form the EU's institutional framework for digital governance, addressing challenges in the digital age.

- **EU institutions**

The primary EU institutions responsible for digital governance are the European Commission (EC), the European Council, and the European Parliament (EP). The EC is the EU's politically independent executive arm, responsible for proposing new European legislation and implementing decisions of the EP and the Council.[25] Regarding EU digital governance, the EC internally provides the framework for its management, control, and monitoring. For example, in 2021, the EC proposed a policy framework to support national governments to achieve the Digital Decade targets by 2030, focusing on infrastructure, technology uptake, and e-governance.[26] Moreover, the Commission ensures attention to

[25] European Union. "Institutions: European Commission." https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission, Accessed: 12 Nov 2023.
[26] European Commission. "Europe's Digital Decade." https://digital-strategy.ec.europa.eu/en/node/157/printable/pd f.

digitization topics through publications such as communications, action plans, and recommendations, while proposing initiatives. Externally, the EC represents the EU and advocates for international cooperation and standards-setting on digital governance issues, engaging with other countries, organizations, and partners through ongoing dialogue.

Both the European Council and the EP are crucial in establishing the EU digital agenda. The Council sets the EU's direction and political priorities, addressing complex issues requiring higher levels of intergovernmental cooperation. In 2023, the Council sets out priority actions for stronger EU action in global digital affairs, urging both the EU and its Member States to reinforce their role and leadership. It stresses that in order to bring its digital diplomacy to the next level, the EU needs to act in a "Team Europe" approach, jointly protecting its strategic interests.[27] To its credit, the Council lays the foundation for common EU external action on digital governance issues. The EP, on the other hand, beginning as a Common Assembly in 1952, has gradually transformed into today's co-legislator with powers nearly equivalent to those of the Council. It is crucial in responding to legislative proposals on digital governance from the EC. Generally, Members of the EP (MEPs) tend to propose minor amendments instead of introducing creative or disruptive ideas. Despite this tendency, the EP's extended legislative powers and intellectual freedom of its MEPs facilitate its open and pragmatic debating culture, enabling it to craft a balanced and comprehensive EU digital agenda.

- **EU bodies**

[27] Council of the EU. "Digital diplomacy: Council sets out priority actions for stronger EU action in global digital affairs", European Council, https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/digital-diplomacy-council-sets-out-priority-actions-for-stronger-eu-action-in-global-digital-affairs/, Accessed:15 Dec 2023.

Besides the institutions, two specialized EU bodies focus on specific tasks in digital governance: the European Data Protection Supervisor (EDPS) and the European Data Protection Board (EDPB).

EU institutions process citizens' personal information, involving activities like collecting, recording, storing, or sending data. It is the task of the EDPS to uphold strict privacy rules that govern these activities. For instance, the Annual Report 2020 highlights the EDPS's oversight of data protection during the COVID-19 pandemic, including the formation of an internal working group to assess government and private sector responses.[28] Throughout 2020, this EDPS monitored developments and prepared for the future of data protection and privacy after the pandemic. Additionally, it advises EU institutions and bodies on personal data processing, related policies, and legislation. Collaborating with national authorities of EU countries, it ensures consistency in data protection.[29] Overall, the EDPS prevents the violation of human rights in EU digital governance process, preserving trust in EU digital policies.

On the other hand, the EDPB, established in 2018, has a broader mandate to enhance the effectiveness of EU law in digital governance. It ensures consistent application of EU law in this field, particularly the GDPR and the Data Protection Law Enforcement Directive, across all covered countries. The EDPB provides general guidance, including guidelines, recommendations, and best practices, to clarify the GDPR. It adopts consistency findings to

[28] European Data Protection Supervisor. "ANNUAL REPORT 2020", *European Unio*n, 2021, https://edps.europa.eu/system/files/2021-04/2021-04-19-annual-report-2020_EN.pdf, Accessed: 16 Dec 2023.
[29] European Union. "European Data Protection Supervisor (EDPS)", https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-supervisor-edps_en, Accessed, 18 Dec 2023.

ensure a consistent interpretation of the GDPR by all national regulatory bodies.[30] Besides, the EDPB works to foster cooperation among national data protection authorities.

Together, these bodies contribute to establishing a strong framework for data protection, privacy, and digital governance within the EU.

- **Decentralized agency**

There are currently over 30 decentralized agencies in the EU, each with their own legal personalities. These agencies support EU policy implementation by fostering collaboration between EU institutions and national governments. Among these agencies, the European Union Agency for Cybersecurity (ENISA) plays a key role in EU digital governance.

Strengthened by the 2019 EU Cybersecurity Act, ENISA's focus is now on bolstering cybersecurity capabilities and cultivating a secure digital environment across EU Member States. It enhances the EU's cyber policy by developing cybersecurity certification schemes to instill trust in digital products, services, and processes. This agency collaborates with EU countries and bodies, addresses emerging cyber challenges, and assists Member States in managing cybersecurity incidents. It also supports the coordination of the EU in case of large-scale cross-border cyberattacks and crises. In addition, the agency also works with organizations and businesses to enhance trust in the digital economy, fortify EU infrastructure resilience, and ensure the digital safety of citizens. This is achieved through knowledge-sharing, staff and structure development, and awareness-raising initiatives.[31]

[30] European Union. "The European Data Protection Board (EDPB)", https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_en, Accessed, 18 Dec 2023.
[31] European Union. "European Union Agency for Cybersecurity (ENISA)", https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en, Accessed, 18 Dec 2023.

2. Effects

EU institutions, bodies, and agencies have been vital in building trust among Member States to improve the implementation of EU digital governance. Institutional trust within these institutions and related regimes promotes cooperation, coordination, information sharing, transparency, and the development of mutual interests.

Liberal institutionalism provides a systematic explanation of how international institutions influence cooperation and the establishment of trust mechanisms. It contrasts with other perspectives, such as realism, which focuses more on power politics and national interests, viewing the struggle for power as the essence of the international community.[32] Liberal institutionalism places greater emphasis on the potential for cooperation in an anarchic international system. Initially, the focus on international institutions is apparent in "Power and Interdependence", where detailed discussions on maritime and monetary regimes mark the inception of liberal institutionalism's development.[33] In the early 1980s, Keohane critiques the fundamental perspective of realist scholars such as Gilpin in "After Hegemony", stating that international institutions established during hegemony can sustain cooperation even after hegemony.[34] Therefore, the international institutions are actually driven by the states' need to cooperate. "Cooperation under Anarchy" in 1986 centers on the possibilities and conditions for rational state actors to cooperate in international anarchy, with a particular emphasis on the influence of international institutions and regimes.[35] Later, the release of "International

[32] Morgenthau, Hans Joachim. *Politics among Nations*. 5th ed., Knopf., 1973, pp.118-121; Waltz, Kenneth Neal. *Theory of International Politics.* McGraw-Hill, 1979, pp.88-93.
[33] Keohane, Robert O. (Robert Owen), and Joseph S. Nye. *Power and Interdependence*. 4th ed., Longman, 2012, pp.55-139.
[34] Keohane, Robert O. (Robert Owen). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press, 1984.
[35] Oye, Kenneth A. *Cooperation under Anarchy*. Princeton University Press, 1986.

Institutions and State Power" marks the maturation of liberal institutionalism. Keohane theorizes essential questions regarding the conditions for international cooperation, the role of international institutions in cooperation, and the relationship between states and international regimes.[36] The international institutions are recognized as a determinant of state behavior.

Based on liberal institutionalism, in a state of anarchy, international institutions play a crucial role in the establishment of institutional trust among states. Liberal institutionalism defines international institutions as a comprehensive, interconnected system of formal and informal rules, which manifest in three forms: 1) formal intergovernmental or cross-national nongovernmental organizations with distinct rules and charters; 2) international regimes refer to institutions with explicit rules, agreed upon by governments, that pertain to particular sets of issues in international relations; 3) and conventions, informal institutions with implicit rules and understandings, that shape the expectations of actors.[37] According to liberal institutionalism's definition of international institutions, three key characteristics can be summarized. Firstly, although not as binding and mandatory as domestic laws, international institutions are authoritative. Acknowledged as rules by members of the international community, they serve as a code of conduct in specific fields, contributing to their effectiveness in most cases. Secondly, international institutions are constraining. It relies on the fact that it enables rational and self-interested states to better pursue their national interests and avoid common losses. Finally, international institutions are interrelated. The development of international institutions results in the interconnection of institutions across various issues,

[36] Keohane, Robert O. *International Institutions and State Power: Essays in International Relations Theory*. 1st edition, Routledge, 2020, pp.1-20.
[37] *Ibid.* pp.3-4.

forming a networked system. Based on the characteristics, it can be concluded that the non-cooperative behavior of states in international interactions is a result of trust deficit, which results in high transaction costs, preventing the realization of cooperation that would otherwise be mutually beneficial for both parties.[38] In this context, on the one hand, international institutions can provide high-quality information and a standardized framework for norms of conduct. This, in turn, enables states to gain a clearer understanding of each other's realities and intentions. On the other hand, due to the interrelated nature of the international institutions, deliberate or intentional violations of them will result in an unsustainable increase in transaction costs for the state. As a result, due to the service and punitive nature of institutions, it is possible to form a relationship of trust in the international community and to establish trust mechanisms in dealing with common global issues. The presence of international anarchy does not necessarily lead to disorder in the international community.[39]

The EU has succeeded in establishing institutional trust in the field of digital governance in the region. The EU consists of Member States with varying levels of development, preferences, and national interests, but without exception, each member state is a self-interested and rational international actor. Their primary concern is to address conflicts of interests between states in a way that minimizes costs and maximizes benefits for each member state. In the digital era, however, issues caused by digital technology have surpassed traditional national boundaries and evolved into common global concerns. Cooperation has become the most effective way of digital governance for Member States. Premised on shared national

[38] Yaqing, Qin. *Power, Institutions, and Culture*, 2nd edition, Peking University Press, 2016, p. 105.
[39] Keohane, "Institutional Theory and the Realist Challenge after the Cold war," *Neorealism and Neoliberalism*, ed. by Baldwin, p.269.

interests, the EU has provided more unified policies and strategies for digital governance through a supranational approach, providing a valuable model for cooperation on this global issue. Especially the EU supranational entities play a crucial role in forming institutional trust among Member States by establishing common norms and expectations. The EC's policy formulation for digital governance ensures a level playing field, consistent rule application, reflects institutional authority, and enhances Member States' confidence in policy effectiveness. The Council represents Member States at the ministerial level in discussions and negotiations on digital governance. The collaborative nature of these interactions helps to build regional trust mechanisms by ensuring that decisions align with the interests and concerns of individual Member States. The EP, representing the interests of EU citizens, fosters cooperation and enhances trust through its transparent and inclusive approach. The broad participation of elected representatives and the acceptance of diverse views from Member States in the decision-making process contribute to increased willingness to cooperate. Other EU bodies and agencies, including the EDPB, the EDPS, and the ENISA, with a focus on digital governance bring expertise, share high-quality information and technology, and strengthen the foundations of trust mechanisms by providing authoritative perspectives on complex digital issues. Together, the norms and standards developed by these EU supernational institutions create a predictable environment for Member States and thus diminish political uncertainty.

In conclusion, at a time when global digital governance is struggling to make progress, the EU has successfully established a significant level of trust within the region. This trust is essential for the effective implementation of digital governance measures and the successful functioning of the EU’s digital ecosystem.

3. Challenges

While the EU leads in supranational digital governance, it still faces challenges. Its trust-building model could be perceived as "digital protectionism" and meet opposition internationally. Moreover, the coexistence of EU-led supranational digital governance and member state-led traditional governance has implications for institutional trust.

To establish an effective environment for digital governance, the EU is more likely to adopt measures that may be perceived as discriminating against foreign market participants, including antitrust. The conflict over data protection initially manifested in transatlantic relations between the EU and the U.S. EU regulators have taken aggressive action against U.S. technology companies for years, levying or threatening billions of euros in fines on Intel, Microsoft, Google, and Amazon under the banner of securing EU "digital sovereignty".[40] Meanwhile, the U.S. has closely monitored the EU's digital governance initiatives, labeling certain policies indiscriminately as "digital protectionism". The U.S. has pressed the EU to alter its behavior to uphold open digital networks and thus ensure its own dominance in global digital governance. The EU's ambition to lead in digital governance has increased tensions with the U.S. Therefore, Member States may exhibit diminished trust in the EU's supranational digital governance, given the pressure from the U.S. on EU's overall digital governance institutions.

There is also a tension between EU-led supranational forms of digital governance and member state-led traditional forms of governance. The flip side of the civic European identity

[40] Barshefsky, Charlene. "EU Digital Protectionism Risks Damaging Ties with the US." *FT.Com*, 2020. https://www.proquest.com/docview/2476216082?parentSessionId=EqfmRdbS9T%2Fylvlqjhk4RWuXWbkCVi%2FXPL9OSvlxbTY%3D&pq-origsite=primo&accountid=14701&sourcetype=Trade%20Journals#center, Accessed: 25 Dec 2023.

is the "ethnonationalist" side of Europe: an essentially ethnic-based version of European identity that excludes certain groups from the vision of Europeanness.[41] Member States' attitudes toward EU digital governance depend on benefits and alignment with EU norms. If a member state doesn't benefit and holds skepticism about EU norms, it may support traditional government-led governance, challenging trust mechanisms. For example, regarding to EU digital governance, France emphasizes safeguarding technology security and preserving the digital sovereignty of the entire EU. In contrast, the central and nordic countries prioritize nurturing their own national digital economy centers and seek improved EU coordination in the digital marketplace to facilitate the growth of their startups. Therefore, the achievement of EU supranational digital governance requires, in particular, compromises among Member States. EU legislation needs to consider the balance between the positions of Member States.

To address these challenges, the EU should prioritize open communication, inclusive decision-making, and flexibility in digital governance. Balancing supranational benefits with respect for national interests and global trade dynamics is vital for building trust.

[41] Fligstein, Neil, et al. "European Integration, Nationalism and European Identity." Journal of Common Market Studies, vol. 50, no. s1, 2012, p. 113.

Chapter IV：EU Digital Governance and Institutional Trust

In the following discussion, institutional trust is classified into two categories: (1) basic forms of trust mechanisms based on the roles and functionality of institutions and (2) a potential trust mechanism in the future with a focus on collective interests and individual rights. The exploration will delve into the influencing factors shaping these trust mechanisms.

1. Basic Forms of Institutional Trust in the EU Digital Governance

Building upon the previous argument, trust in EU digital governance primarily manifests as institutional trust. Basic trust mechanisms can be delineated into two forms: (1) compulsory trust mechanism and (2) favorable trust mechanism. These two trust mechanisms are considered basic forms of institutional trust because they directly stem from the functions and roles of the institutions themselves. The former is defined based on the functioning of the institutions, while the latter is defined by the will of the Member States themselves under the institutions. They are interdependent, each relying on the other. However, differences exist between the two basic trust mechanisms. The compulsory trust mechanism emphasizes passive trust by compelling Member States to trust each other based on the roles and functions of institutions. In contrast, the favorable trust mechanism emphasizes active trust. It highlights Member States' willingness and need to trust based on the benefits the institutions can bring.

1.1 Compulsory and Favorable Trust Mechanisms

- **Compulsory Trust Mechanism**

In the social structure, trust is confidence in the fulfillment of role expectations and the various forms of sanctioning mechanisms that ensure such performance.[42] "Sanctioning

[42] Seligman, Adam B. *The Problem of Trust*. Princeton University Press, 1997, p.25.

mechanisms" here refer to the consequences individuals face for adhering to or deviating from norms. At the EU supranational level, these mechanisms are integrated into the EU institutional system, fostering compulsory trust mechanism among Member States.

From an institutional perspective, regulations are enforced through punishment, ensuring adherence by Member States. The effective implementation of compulsory trust mechanism relies on both the vertical and horizontal effects of the institutions. Vertically, a state's violation of the institutions is not viewed as an isolated act but rather as part of a series of collaborations in the same problem. While it may yield short-term benefits, the cost of such short-term behavior is damage to the state's reputation. Horizontally, interconnected institutions in various areas create an extensive network. States acting against one institution may face penalties in other areas of cooperation.[43] It is the institutions reinforcement of the role of future influence that compels states to conform to the supranational system, creating a compulsory trust mechanism. Furthermore, the compulsory trust mechanism is rooted in the legitimacy of the system. The concept of political legitimacy refers to some benchmark of acceptability or justification of political power or authority and obligation.[44] It implies the right and acceptance of an authority, usually a governing law or a regime. The main function of legitimacy is precisely to justify coercive power. Recognition of the system's legitimacy by Member States leads to their compliance with the relevant institutions.

The EU is dedicated to promoting cooperation and coordination among Member States across various issue areas, including the economy and trade, security and defense, environment, and migration. Violations of EU regulations in the field of digital governance by Member States

[43] Yaqing, Qin. *Power, Institutions, and Culture*, 2nd edition, Peking University Press, 2016, p.102.
[44] Peter, Fabienne, "Political Legitimacy", *The Stanford Encyclopedia of Philosophy* (Winter 2023 Edition), p.5.

can impede cooperation in other issue areas. Therefore, one of the forms of the EU trust mechanism for digital governance is compulsory, meaning that the relevant institutions apply uniformly to all Member States. This ensures consistent standards and obligations in the digital governance, forming the basis for shared compliance among Member States. While compulsory trust mechanism plays a crucial role, it is essential to pay attention to ensuring the transparency and fairness of the policy formulation process. This ensures that the interests of Member States are fully respected and balanced.

- **Favorable Trust Mechanism**

Favorable trust mechanism, one the other hand, emphasizes a state's need to prioritize its self-interest. It refers to a mechanism of mutual trust and cooperation established by states based on their own socio-economic development and motivated by their own willingness and necessity for collaboration, recognizing the benefits that institutions can bring.

National interests serve as guiding principles for state behavior, including security, political, economic, and cultural considerations. Among these, the most important are national security interests, which pertain to the survival of the state. Realism asserts that conflicting interests among states are inherent to international society due to divergent state interests. Each state views its own interests as supreme, making conflict mediation impossible.[45] However, while the use of force is an option for resolving conflicts, the cost of such a solution is extremely high. A rational state will demand and join international institutions if those institutions can provide net benefits relative to the outcome if no agreement to join is reached.[46]

[45] Morgenthau, Hans Joachim. *Politics among Nations*. 5th ed., Knopf., 1973, pp.118-121.
[46] Keohane, Robert O. (Robert Owen). *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton University Press, 1984.

These benefits include reduced transaction costs, increased information flows, and diminished uncertainty. By fulfilling these functions, institutions enable states to negotiate mutually beneficial agreements that would otherwise be unattainable. Therefore, states need to cooperate for their own sake, and conditions for cooperation do exist in the international community.[47]

In today's world, non-traditional security issues pose significant challenges to the survival and well-being of peoples and states. These issues include climate change, resource scarcity, infectious diseases, and more. The development of digital technologies also falls under non-traditional security and may jeopardize national security. For instance, EU digital development has increased the risk of cyberattacks and data breaches. Government and critical infrastructure networks, including power, water, and transportation, are threatened. Additionally, the ease of spreading disinformation poses risks of social unrest, political interference, and social fragmentation, thereby threatening the political stability of Member States and EU cohesion. The urgency of digital governance, coupled with the realization that the cross-border nature of data usage makes it impractical to address the issue solely at the member state level[48], have fostered a common will and political commitment to solidarity among Member States. Therefore, favorable trust mechanism for EU digital governance represents a voluntary form of mutual trust among Member States, established based on their necessity and willingness to address various challenges arising from digital technologies.

[47] Yaqing, Qin. *Power, Institutions, and Culture*, 2nd edition, Peking University Press, 2016, p.95.
[48] European Commission. "Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), *Brussels*, 2022, p.7.

1.2 Analysis of Influencing Factors

Liberal institutionalism argues that for peace in international affairs, states must cooperate and yield some sovereignty to create "integrated communities", fostering economic growth and addressing security issues.[49] Therefore, market economics and regional security factors can be seen as reasons for the initial establishment of two basic trust mechanisms. These two factors are significant in establishing institutional trust for EU digital governance.

- **Market Economic Factor**

The development of digital market economy can enhance capital and labor productivity, reduce costs, and get access to global markets.[50] These commercial benefits drive cooperation among EU Member States, promoting digital market integration and thereby fostering trust. However, varying levels of economic development present challenges to trust-building.

Despite the evolution of the global digital economy, the EU not only lacked a cohesive digital development plan but also caused internal conflicts, leading to a relatively low level of digitization across the entire EU.[51] This placed the EU in a passive position within the rapidly advancing digitization landscape. As a result, the commercial benefits of the development of the digital economy have become the main driving force behind the formation of trust mechanisms in the EU digital governance. In May 2015, the EU introduced the Single Digital Market Strategy, empowering consumers and businesses to maximize their use of digital goods and services across EU countries.[52] This aligns with the shared objective of EU Member States

[49] Baylis, John, et al., editors. The Globalization of World Politics: An Introduction to International Relations. Eighth edition., *Oxford University Press*, 2020, p.213.
[50] Carl Dahlman, et al. "Harnessing the Digital Economy for Developing Countries." *OECD Development Centre Working Papers*, Organization for Economic Co-Operation, and Development (OECD), 2016.
[51] Na, Yang, and Hongyi, Chen. "Issue Spillover and Form Transformation: Understanding European Integration from the Dynamic Perspective", *European Studies*, Vol. 41, No. 2, 2023, p.14.
[52] European Commission, "A Digital Single Market for Europe， " 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192, Accessed: 10 Jan 2024.

to establish an internal market and economic union within the EU borders. Consequently, the EU introduced successive measures like the Digital Services Act in 2020 and the Digital Markets Act in 2022 to institutionalize these objectives.

However, the uneven level of development in the digital economy among Member States has resulted in conflicts of common interests, thereby adversely impacting the construction of trust mechanisms. Some countries may prioritize the protection of their businesses and industries, while others may lean towards fostering the prosperity of the digital economy through openness and cooperation. Taking the example of Finland, with its more advanced digital economy, and Romania, which lags behind, it is evident that Finland places a strong emphasis on innovation, digital public services, and a robust start-up ecosystem. In contrast, Romania still focuses on promoting entrepreneurship and developing digital infrastructure. These divergent interests may result in challenges in coordinating on key issues, and thus impede the formation of trust mechanisms.

- **Regional Security Factor**

In political science, governance issues, not threatening state survival, are termed “low politics”. Conversely, vital matters like national and international security are labeled "high politics." Digital governance straddles both, involving economic interests and significant security implications. The field of digital governance in the EU is characterized by the proliferation of supranational forms of governance from lower to higher political issues.[53]

As described earlier, the evolution of the digital economy involves extracting information from vast datasets and controlling that data. This not only signifies economic gains but also

[53] Na, Yang, and Hongyi, Chen. p.1.

embodies a form of informational and discursive power. The EU has recognized the disruptive potential and transformative impact of new technologies on the security and defense landscape, including autonomous robotics and artificial intelligence. These technologies have significant civil-military applications, bridging both the economic and defense spheres. However, in the context of the rapid global development of the digital economy industry and technology, EU Member States find themselves in a relatively weaker position compared to digital technology powerhouses like the U.S. and China. There is a higher dependency on the digital economy and related technology from outside the region. In the event of differences and conflicts, the repercussions extend beyond economic losses, posing a potential threat to the security of the region. Therefore, the digital technology contributes to the emergence of a cross-sectoral European security landscape, and the transformation of the EU into a high-tech powerhouse via new configurations of power relations in the case of future-oriented technologies.[54]

As individual EU Member States find themselves incapable of effectively addressing the confrontation of external digital technologies and potential national security threats arising from digital attacks, they have recognized the importance of ensuring the security in the EU digital domain. A notable effort in this direction is the Network and Information Systems Security Directive (NIS Directive), which came into force in 2018. The directive aims to enhance overall cybersecurity in the EU by fostering a culture of risk management, cooperation, and information sharing among Member States. Additionally, the EU is actively developing a unified approach to address the security risks associated with 5G technologies, emphasizing the need for a coordinated response to safeguard critical infrastructure. Meanwhile, the EU

[54] Csernatoni, Raluca. "The EU's Technological Power: Harnessing Future and Emerging Technologies for European Security." *Peace, Security and Defence Cooperation in Post-Brexit Europe*, Springer International Publishing, 2019, p. 119.

engages with Member States to strengthen their capacity to respond to cyber threats and enhance overall cybersecurity posture. In conclusion, digital governance has emerged as a critical aspect of EU Member States, representing their most strategic national interests.

2. Prospects for a More Robust Trust Mechanism in the Future

Due to the functionality of institutions and states' reliance on them, compulsory and favorable trust mechanisms have ensured the smooth implementation of EU digital governance at the supranational level. However, institutional trust still has room to development. Trust mechanisms should not solely rely on its effectiveness in serving individual states' interests and benefits. It should also reflect the moral incentives of Member States to realize the collective interests of the EU as a whole and meanwhile embodies human rights when obeying the EU institutions. A more robust trust mechanism, defined here as solidarity-based trust mechanism, will require ongoing efforts to deepen in the future among Member States.

2.1 Solidarity-based Trust Mechanism

The fundamental emphasis of liberal institutionalism lies in the cooperation over conflict and downplays power structures.[55] It is a continuation of the Western liberal tradition, demonstrating a strong sense of fraternity and optimism. However, what the liberal institutionalism has overlooked is that institutions serve to preserve a certain system within the society, i.e., the institutions represent political and economic system while ignoring the shared values and spontaneous solidarity embodied in the system.

[55] Keohane, Robert O. *International Institutions and State Power: Essays in International Relations Theory*. 1st edition, Routledge, 2020. pp.10-11.

In fact, the theoretical foundation of liberal institutionalism has always been rooted in advocating for human rights values such as liberty, equality, and fraternity. For example, John Locke envisions an ideal society where human rights are respected, and all people are considered equal. Individual rights are inherent to individuals and cannot be transferred or revoked by others.[56] By contrast, the rights of collectivities are artificial, because the structure of human groupings, unlike the structure of groupings of animals lower on the evolutionary scale, are not given by instinct but are constructed.[57] Therefore, the individual is paramount; the state is secondary, serving as a means to an end.

In the context of the EU, however, the development of European rights and values has extended beyond individual rights since the signing of the European Convention for the Protection of Human Rights and Fundamental Freedoms in 1950. Indeed, the values of European constitutionalism, most notably the triad of human rights, rule of law, and democratic procedures, encompass collective rights and guarantees of institutions.[58] Article 2 of the Treaty on EU acknowledges values that refer to economic conditions and societal relations, especially solidarity (European Union, 1992/2002). When regulators fail to enforce existing regulations based on solidarity, both individual and collective rights, as well as institutions, will be eroded.

Therefore, solidarity-based trust mechanism refers to the cultivation of international institutions and state relations towards peace and humanity by ensuring the maximum realization of individual rights based on collective rights and solidarity among states. This represents the direction institutional trust within liberal institutionalism should evolve in the

[56] Leiter, Yechiel M. *John Locke's Political Philosophy and the Hebrew Bible.* Cambridge University Press, 2018.
[57] Brown, Seyom. *International Relations in A Changing Global System: Toward A Theory of The World Polity*, Second Edition. Second edition., Taylor and Francis, 2018, p.95.
[58] Zygmuntowski, J. J. & Zoboli, L. & Nemitz, P. F. "Embedding European values in data governance: a case for public data commons". *Internet Policy Review*, 2021, 10(3), p.4.

future, i.e., emphasizing the value that institutions inherently contribute to solidarity and the collective interests. Despite the cultural diversity among EU Member States, the EU can be able to foster consistent cooperation and consensus in various areas by emphasizing the shared value of solidarity, characterized by collective rights and the public interests, within its institutions. However, building solidarity-based trust is not an overnight process. It requires considerable time for Member States to accept and internalize this shared value.

2.2 Analysis of Influencing Factors

The European identity serves as a motivating force, urging Member States to be part of a collective endeavor to advance the Union as a whole. Conversely, discrepancies or suspicions regarding shared values can impede progress in digital governance.

The concept of "European identity" first appeared in the Document on European Identity signed by the original EU countries, pointing out "the nine European states might have been pushed towards disunity by their history and by selfishly defending misjudged interests. But they have overcome their past enmities and have decided that unity is a basic European necessity to ensure the survival of the civilization which they have in common."[59] The concept of "European identity" thus reflects the Member States' efforts to transcend historical interrelationships and build trust by prioritizing the integration of European societies. This helps to form a distinctive culture and institutional system that appeals to them as legitimate.

A member state's stance on European identity positively correlates with its acceptance of EU governance. On the one hand, European identity determines whether nation-states

[59] Bulletin of the European Communities, "Declaration on European Identity," *Luxembourg: Office for official publications of the European Communities*, 1973, No 12., p.118.

acknowledge their EU membership, voluntarily accept the EU political order, and align their behavior with EU supranational laws and rules.[60] In other words, the acknowledgment of the EU identity promotes solidarity and trust among Member States. On the other hand, a shared European identity is vital in increasing the effectiveness and legitimacy of EU institutions. Higher levels of integration amongst the EU states, which have expanded beyond the initial economic dimension into the political and social sphere of activity, serve as a dual reminder of the benefits and potential pitfalls of European interconnectedness.[61] The effective EU digital governance requires Member States to reach agreements at the supranational level.

Conversely, if a member state adopts a skeptical attitude towards European identity, it can lead to a trust crisis. A significant example is the impact of Brexit on EU digital governance. Despite UK membership in the EU, there has been historical ambivalence and reluctance toward European integration, fueled by concerns over national identity. The UK's inherent distrust prompted the Brexit vote, resulting in a loss of regulatory capacity and a new digital governance architecture in the UK.[62] With the UK's departure, the EU must adopt a more hands-on approach to regulate the digital sector, aiming to promote European champions while limiting the influence of US companies. Identity disagreements negatively affect EU harmonization policies and governance effectiveness, compromising its global competitiveness in the digital domain.

---

[60] Wiener, Antje, et al., editors. *European Integration Theory*. Third Edition., Oxford University Press, 2019, p.148.
[61] Shehaj, Albana. "How Is a European Identity Significant to the Future of the European Union?", *Open Democracy (London)*, 2015, Retrieved from https://login.proxy.bib.uottawa.ca/login?url=https://www.proquest.com/magazines/how-is-european-identity-significant-future-union/docview/1684293873/se-2.
[62] Harcourt, Alison. *Brexit and the Digital Single Market*. First edition., Oxford University Press, 2023.

Given the multi-ethnic composition and political controversies within the EU, while a common European identity can have a unifying effect, it still requires ongoing active interaction and bonding among member states a long-term future.

3. Conclusion

To sum up, in terms of EU digital governance, relatively well-developed supranational institutions already exist in the EU. Ensured by the EU's robust institutional framework, two kinds of basic trust mechanisms can be observed in EU digital governance: compulsory trust mechanism and favorable trust mechanism. On one hand, the role of institutions itself has mandatory nature, compelling Member States to trust each other passively in digital governance. On the other hand, the benefits and interests brought from institutions motivate Member States' demand and willingness for forming proactive trust among them. Both trust mechanisms are essential for cooperation in EU digital governance. In addition, the market economy and regional security, which are the most important parts of the national interests, also affect the EU trust relationships to varying degrees.

The prospected trust mechanism, the solidarity-based trust mechanism, is still under the framework of institutional trust but with an emphasis on selflessness, a sense of morality, and a duty to serve humanity. This trust mechanism is not profit-driven by a single nation but rather based on the consensus on safeguarding collective interests and individual rights. However, this trust mechanism is far from mature and requires ongoing internalization of common identities and shared values among Member States. The EU is still progressing towards the establishment of a solidarity-based trust mechanism for the future.

Chapter V: A Case Study of the GDPR in the Context of Covid-19 Pandemic

The introduction of GDPR in 2018, coupled with the EU's utilization of digital governance during the subsequent Covid-19 pandemic, serves as a clear illustration of the institutional trust mechanisms in EU digital governance. This chapter will also provide a brief analysis of the influencing factors and their impact on the trust mechanisms.

1. Case Background

The contemporary digital paradigm, marked by a drastic surge in data consumption and breaches, poses a threat to individuals' privacy. In response, the EU introduced the GDPR to establish robust privacy protection for its Member States. The GDPR applies to organizations worldwide that target or collect data related to individuals in the EU, focusing on key aspects such as data storage, processing, collection, and disclosure. Enforced on May 25, 2018, after passing the EP in 2016, it stands as the world's strictest privacy and security law. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.[63]

The outbreak of the Covid-19 pandemic in late 2019 and early 2020 has led to a global health crisis impacting countries worldwide. Throughout the past year, governments in the EU have dedicated substantial efforts, through research and their overall healthcare systems, to comprehensively understand and contain the pandemic. As highlighted by academics, a vital source of information is the amount of digital health data that can be collected, and a guaranteed way to achieve this is through collaboration among Member States and international health

[63] Wolford, Ben. "What is GDPR, the EU's new data protection law?", *GDPR EU*, https://gdpr.eu/what-is-gdpr/. Accessed: 21 Jan 2024.

research efforts.[64] In an attempt to gather information as quickly and efficiently as possible, an effort has been the creation and operating of contact tracing applications and other digital health tools which enable the gathering of personal data and sensitive information, posing a huge challenge to data protection in the EU.[65] This situation gives rise to questions surrounding the ethics of using citizens' data in a seemingly broad manner. It places the public interest and the privacy of individuals on opposite ends of the scale, challenging the common principles and values in the EU.

In response to this crisis, the GDPR serves as the framework for EU digital governance, providing the necessary legal structure to manage the handling and processing of personal data. It ensures that these processes are lawful, fair, and aligned with the interests of Member States.

2. Analysis of Trust Mechanisms

2.1 GDPR and Basic Institutional Trust Mechanisms

The effective implementation of the GDPR within the EU during the pandemic reflects the relatively robust institutional trust mechanisms developed by EU Member States in digital governance. On one hand, compulsory trust mechanism relies on the coercive power of EU institutions to promote member states to process data while protecting personal data privacy. On the other, it offers effective safeguard for Member States to develop contact tracing and alerting apps to contain the spread of virus and protect regional security, reflecting a favorable trust mechanism.

---

[64] McLennan, Stuart, et al. "COVID-19: Putting the General Data Protection Regulation to the Test." *JMIR Public Health and Surveillance*, vol. 6, no. 2, 2020, p.279.

[65] European Commission. "2020 Mobile Contact Tracing Apps in EU Member States." December 18, 2020. https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/trav-el-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en. Accessed: 21 Jan 2024.

- **Compulsory Trust Mechanism**

As virus transcends national borders, the EU's GDPR digital legislation establishes mandatory regulations, fostering compulsory trust mechanism among Member States to strengthen collaborative efforts in handling digitally sensitive information. This regulation has successfully promoted a coordinated response to Covid-19 outbreaks through mutual trust.

In principle, the GDPR provides a toolset for the processing of personal data in a health crisis, including for health-related research.[66] For example, in 2(i) of Article 9 of the GDPR, it is stated that processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.[67] This establishes legislative principles and a legal framework for processing personal data during a pandemic. It ensures flexible cooperation between the public and private sectors of EU Member States during the crisis, prevents improper processing of private information by other states, and encourages Member States to foster trust in digital security, emphasizing research and collaboration on pandemic-related issues. Furthermore, the EU body—EDPB, responsible for ensuring the consistent application of the GDPR in the EU and cooperation between all Data Protection Authorities (DPAs), issues guidance on GDPR implementation in Member States

[66] European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. 2020 Apr 21. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf, Accessed: 25 Jan 2024.

[67] European Council, "GENERAL DATA PROTECTION REGULATION (GDPR) - Official Legal Text", Article 9-2(i), https://gdpr-info.eu/art-9-gdpr/, Accessed: 24 Jan 2024.

during this period. Besides, The EU parliament stressed that any digital measures against the pandemic must conform with current data protection and privacy legislation.[68] This collaborative effort of supranational bodies successfully enhances the effective implementation of GDPR regulations.

- **Favorable Trust Mechanism**

The EU faces challenges in the initial stages of fighting the virus and swiftly emerged as the epicenter. To curb the pandemic's spread, the EU collaborates with Member States to devise effective solutions. Within the GDPR framework, the Member States and the Commission jointly launch contact tracing and alerting apps for national security interests, successfully forming a favorable trust mechanism.

COVID-19 was fought in the digital age. It disrupts global trade, employment, and travel, and many governments have to take strict measures to control the spread of the virus and minimize the burden of morbidity and mortality so that health care systems remain functional.[69] To control the spread of coronavirus, cooperation and digital information sharing among Member States are essential. At the beginning of the pandemic, 22 public health authorities of EU Member States launch national tracing and warning apps as part of a package of measures. In October 2020, European countries and the EC established the European Federation Gateway, enabling interoperability among national tracing apps. This facilitates more efficient and coordinated surveillance, prevention, treatment, and overall public health management, crucial

[68] Schneble, Christophe Olivier, et al. "Data Protection during the Coronavirus Crisis." EMBO Reports, vol. 21, no. 9, 2020, pp. e51362-n/a.
[69] Triantafyllidis, Andreas, et al. "Features, Outcomes, and Challenges in Mobile Health Interventions for Patients Living with Chronic Diseases: A Review of Systematic Reviews." *International Journal of Medical Informatics (Shannon, Ireland)*, vol. 132, 2019, p.984.

for combatting highly contagious pandemics. It also means that Europeans could keep using their national apps even when crossing borders and benefit from full interoperability, secured transmission, and minimized information exchanged across the Union.[70] Under the protection of GDPR, these contact tracing and warning apps were used voluntarily, fully respecting users' privacy, and refraining from tracking people's locations. Consequently, the apps have been widely adopted on a voluntary basis in accordance with the GDPR, with over 206 million downloads from 2020 to July 2022. They cover up to 20% of all positive cases in a country, representing tens of millions of active users.[71] This widespread adoption proves beneficial for every Member State engaged in the EU's digital governance.

Analysis of Influencing Factors

As previously analyzed, based on national interests, there are two main drivers for the formation of institutional trust mechanisms for EU digital governance: market economy and regional security factors.

- **Market Economic Factor**

In terms of the impact on compulsory trust mechanism, during the pandemic, there is misuse of national data processing powers. Despite the safeguards provided by the GDPR, the pursuit of market economics still incentivizes companies and organizations in certain countries to exploit the ambiguity of legislative boundaries, seeking access to significant amounts of

[70] European Commission. "How contact tracing and warning apps helped during the COVID-19 pandemic", https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/contact-tracing-and-warning-apps-during-covid-19_en, Accessed: 25 Jan 2024.
[71] *Ibid.*

personal data for commercial or economic advantage. This raises data privacy and ethical concerns that challenge the implementations of EU institutions.

As for the impact on favorable trust mechanism, due to the loss of economic interests, there is a tendency for states to prioritize national interests over EU interests to achieve economic recovery. Many countries with below-average GDP per capita, including Spain, Portugal, Greece, Cyprus, and Italy, diverged further from the EU average due to the pandemic. The only exception is the group of new Member States, where even the Baltic countries group in particular converged.[72] Consequently, the condition of the overall market economy during the pandemic is likely to impact EU solidarity and mutual trust among Member States.

However, differences in economic development among Member States is a persistent phenomenon, and reducing disparities between countries and regions is one of the EU's long-term goals. Real convergence has long affected the development of the integration process and the EU's competitiveness in global markets.[73]

- **Regional Security Factor**

Enhancing the security of the EU area further bolsters the EU's compulsory trust mechanism. The EU is not prominently present at the beginning of COVID-19 as public health is neither within the EU's exclusive nor shared competences, and Member States act unilaterally according to their respective national contingency regulations.[74] However, as the crisis unfolded, the EU recognized the need for a coordinated and supranational response to

[72] Abrhám, Josef, and Milan Vošta. "Impact of the COVID-19 Pandemic on EU Convergence." *Journal of Risk and Financial Management*, vol. 15, no. 9, 2022, p.9.
[73] Durkalić, Danijela, et al. "The Measurement of Real Convergence in the EU-28 by Using the Entropy Method." *Economic Časopis*, vol. 67, no. 7, 2019, pp. 698–724.
[74] Roloff, Ralf. "COVID-19 and No One's World: What Impact for the European Union?" *Connections. The Quarterly Journal (English Ed.)*, vol. 19, no. 2, 2020, pp. 25–37.

ensure the well-being of its citizens and the stability of the region. The European Commission's Digital Strategy has gained prominence in the context of the pandemic. Digital tools are employed to monitor and contain the virus's spread, support research, develop diagnostic strategies, treatments, and vaccines, and overall ensure that Europeans remained connected and safe online. Legal access to citizens' digital information under GDPR also becomes vital for Member States to track and control the spread of the virus, as well as to advance vaccine research. This balance between leveraging digital tools for public health purposes and protecting individual privacy became a central consideration in the EU's response.

Furthermore, domestic crises triggered by the pandemic reinforce the necessity for EU digital governance among Member States. The proliferation of socially turbulent online content during the pandemic has emphasized the unprecedented urgency for governments to address the erosion of public trust in political parties. With declining trust in political parties and a rise in support for populist and anti-establishment factions, it's essential for countries to collaborate in the digital sphere to intensify efforts to rebuild trust, address socio-economic disparities, and counter online misinformation and divisive content.

2.2 GDPR and Solidarity-based Trust Mechanism

Protecting privacy right, one of the fundamental human rights, constitutes a crucial aspect of EU digital governance. However, when disease becomes a threat to security, it is difficult to reconcile public health measures and individual rights, but guidance can be taken from understandings of proportionality in the context of personal security. The COVID-19 pandemic has put solidarity into strong focus and emphasis on collective rights is reflected in the GDPR.

- **Solidarity-based Trust Mechanism**

Protecting human rights stands as one of the most important core values of the EU and is protected by the EU Charter of Fundamental Rights. These rights include the right to be free from discrimination, the right to personal data protection, and the right to access justice.[75] The GDPR prioritizes data processing while respecting the rights of the data subject, even in unforeseen circumstances. According to the 2 (j) in Article 9, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.[76] By adopting the relevant provisions of the GDPR, the EU has demonstrated its commitment to fostering a trustworthy, rights-based digital environment in all circumstances.

In the joint statement of 30 March 2020, on the right to data protection during the Covid-19 pandemic, the European Commission stated that data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake.[77] The right to personal data protection under the GDPR is not absolute but must be considered in relation to its function in society, balanced against other fundamental rights. This statement highlights the exceptional circumstance in which individual rights may be derogated from to ensure the protection of collective rights. There exists evidence that in

[75] European Union. "Aims and Values." https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en, Accessed: 25 Jan 2024.
[76] European Council, "GENERAL DATA PROTECTION REGULATION (GDPR) - Official Legal Text", Article 9-2(j), https://gdpr-info.eu/art-9-gdpr/, Accessed: 25 Jan 2024.
[77] Council of Europe, "Joint Statement on the right to data protection in the context of the COVID-19 pandemic", https://rm.coe.int/covid19-joint-statement/16809e09f4, Accessed: 26 Jan 2024.

EU digital governance, solidarity-based trust mechanism already exists to ensure the fullest realization of fundamental human rights by upholding collective rights.

Analysis of Influencing Factors

European Identity factor

The influence of European identity on the GDPR during the pandemic is evident in two ways: the acceptance of GDPR exemption regulations by citizens and the cooperation of Member States under the GDPR framework with the aim of serving the public interest.

The general level of GDPR awareness among European citizens stands at between 69% and 71%.[78] Among these citizens, many accept the secondary use of their data for health-related research under the research exemption of the GDPR, driven by prosocial motivations such as solidarity.[79] Studies have been conducted on the factors influencing citizens' support for GDPR, revealing that such support is linked to values. Recognizing one's EU citizenship correlates with greater trust in institutions and a propensity to endorse selective amendments to the GDPR in exceptional circumstances, even if it means curtailing individual rights to promote solidarity.[80] This indicates that they trust the EU institutions enabling data protection or have faith in their government's handling of data gathered under the framework of GDPR exemption regulation during the pandemic. These EU citizens are under an ethical obligation to share their health information for research purposes to protect public health and safety.

[78] GDPR in 2020 and in the Future: Views from Brussels, Privacy Solved, https://privacysolved-com.translate.goog/gdpr-in-2020-and-in-the-future-views-from-brussels/?_x_tr_sl=en&_x_tr_tl=zh-CN&_x_tr_hl=zh-CN&_x_tr_pto=sc, Accessed: April 8, 2024.
[79] Stuart, et al. p.1.
[80] Richter, Gesine, et al. "Patient Views on Research Use of Clinical Data without Consent: Legal, but Also Acceptable?" *European Journal of Human Genetics: EJHG*, vol. 27, no. 6, 2019, pp. 841–47.

In addition, the availability of GDPR exemption clause, which prioritize the public interest above all else, must be determined by Member State law. (GDPR Article 6[3]) As scientific research on COVID-19 aims to benefit society as a whole, using the legal basis of a task performed in the public interest appears to be a natural choice. At this particular time of crisis, some Member States have demonstrated a state of cohesion and interdependence, particularly emphasizing shared values that prioritize solidarity and collective interests, the primacy of life, and the vital individual rights. In the case of Finland, its decision to join the EU is motivated by a shared vision of forging a new Europe. For a majority of Finns, membership in the EU represented an important way of reviving the economy, promoting national security and preserving the Finnish way of life. Therefore, Finland aligns more closely with the Western identity of EU membership rather than the Eastern identity represented by Russia.[81] During the pandemic, Finland has specified in its national legislation that the public interest legal basis may be relied upon where the processing is necessary for scientific purposes. Germany, a founding member of the EU, as part of an update of its national data privacy legislation, also allows secondary data use without consent for scientific research after appropriate weighing of interests.[82] In this case, both citizens and some of the Member States demonstrate a form of solidarity-based trust by adhering to the EU specific clause on digital governance safeguards during pandemic. This strikes a balance between collective and individual rights while safeguarding the collection of information for public health research in the EU. Solidarity is a European value, and the pandemic is a chance to exemplify it by using

[81] Ingebrigtsen, Christine, and Susan Larson. "Interest and Identity: Finland, Norway and European Union." *Cooperation and Conflict*, vol. 32, no. 2, 1997, p.219, https://doi.org/10.1177/0010836797032002004.
[82] Richter, Gesine, et al. p.842

the GDPR regulatory framework in a way that does not hinder but actually fosters solidarity during the COVID-19 pandemic.[83]

European identity is shared by the Member States in a society typified by pluralism, non-discrimination, tolerance, justice, solidarity and equality between men and women. However, each Member State has specific national identities and histories, and solidarity does not imply the abolition of borders. In times of no major crises, the nation remains the vital framework of political reference for most Member States. Nowadays, the European identity remains a middle path the global and the local, between dilution and self-withdrawal, to avoid, as much as possible, a brutal confrontation between world interdependence and blind, xenophobic, sterile isolation.[84] Therefore, building a complete solidarity-based trust mechanism still requires time and effort.

To sum up, in response to the global health crisis posed by the Covid-19 pandemic, the EU consistently showcases solidarity and trust grounded in shared values and identity to prevent the fragmentation of the EU. Nonetheless, this solidarity-based trust mechanism remains fragile due to national specificities and requires continuous construction in the future.

3. Conclusion

The GDPR stands as the EU's most comprehensive, detailed, and punitive legislation concerning digital governance, and it possesses direct binding authority. Throughout the Covid-19 pandemic, the EU showcases three kinds of trust mechanisms for digital governance under the GDPR framework.

[83] McLennan, Stuart, et al. p.1.
[84] Thierry Chopin, "Europe and the identity challenge: who are we?", *Democracy and Citizenship*, 2018, p.3.

In the basic forms of trust mechanisms, on one hand, it mandates EU Member States to adhere to personal data protection regulations through legislation while granting them access to essential data information in exceptional circumstances, highlighting the role of a compulsory trust mechanism during the pandemic. The coercive nature of the EU institutions and regimes are still effective during the pandemic, highlighting the passive aspect of trust among Member States. On the other hand, the necessity for Member States to prioritize national security and share virus transmission data through tracking and tracing apps emphasizes the significance of cooperation in the favorable trust mechanism. Member States' need for institutions in emergencies emphasizes proactive institutional trust. The effectiveness of the EU system has been challenged and tested during the crisis, demonstrating the sophistication and maturity of EU digital governance system. In this scenario, Member States' national interests influence trust in the mechanism. The pursuit of economic interests somewhat undermines institutional trust, while the protection of regional security strengthens it.

In the solidarity-based trust mechanism, the utilization of the GDPR framework during a pandemic reflects the EU's commitment to collective interests, which restricts certain personal rights during emergencies. During extraordinary times, the presence of a European identity plays a crucial role, enabling the EU to effectively implement digital governance, secure data, and foster trust among Member States based on their shared values, i.e. balancing individual rights while maximizing collective security of life. However, the presence of solidarity-based trust during crisis is not typical, and there remains a distinct sense of national identity within EU Member States. While there is a foundation for a generalized solidarity-based trust mechanism, its development requires ongoing cultivation.

Conclusion

With the in-depth development of digital technology, global digital governance has emerged as a pressing issue for the international community. Currently, the absence of a systemic approach and trust deficit within the global digital governance significantly impede countries from achieving cooperation and establishing regulations in this field. This paper chooses the EU, which is leading the way in digital governance at the supranational level, as the research target, and takes the trust theory as the research framework, analyzes the formation of trust mechanisms of the EU in the field of digital governance, with a view to providing a direction for the practice of global digital governance.

Based on the modes and characteristics of EU digital governance, the paper defines the current EU trust relationship as institutional trust and categorizes it into two types: compulsory trust mechanism and favorable trust mechanism. The compulsory trust mechanism is analyzed based on institutional functionality, relying on the relevant institutions and regulations of the EU in digital governance. It utilizes the coercive force of the mechanism to constrain the behaviors of member states and achieve the goal of institutional trust. Favorable trust mechanism is successfully constructed based on the willingness of Member States to cooperate. Member States commonly agree on the institutional legitimacy and the mutual benefits of cooperation for realizing national interests. Moreover, the market economy and national security are the most important interests of states. These two factors have different impacts on the construction of institutional trust relations regarding to EU digital governance. Market economy factor is related to the significant economic benefits of digital technology as a new factor of production, prompting EU Member States to embrace a supranational form of digital

market integration. Regional security factor has become a fundamental catalyst for the EU to promote trust mechanism construction, with competition in the digital space surpassing traditional geopolitical rivalries.

Furthermore, this paper suggests the potential of a higher level of trust mechanism—the solidarity-based trust mechanism. This trust mechanism is derived from the EU's common value, principles and norms, signifying the acknowledgment by Member States of their belonging to the EU as a unified entity. Under solidarity-based trust mechanism, trust between states is not driven by the coercive nature of the mechanism or the state's interests, but by a spontaneous willingness to help each other. Member States with a stronger sense of identity experience less friction in governance cooperation and are more likely to achieve synergy. While historical conditions and a value base for solidarity-based trust exist among EU member states, the EU has not yet reached such a level of trust in the current era. Therefore, there is potential for solidarity-based trust mechanism to develop further in the future.

Using the implementation of the GDPR framework in the context of Covid-19 pandemic as an example, this paper shows that EU digital governance can still be effective in the face of an emergent event of public health. This case study specifically demonstrates how the institutional trust manifest itself, with the influencing factors of market economy and regional security. In this context, the EU has also demonstrated a degree of solidarity-based trust mechanism, indicating its potential existence. The construction of trust mechanisms in EU digital governance serves as a valuable lesson for the international community. Countries should collaborate to promote the multilateralization of global digital governance rules, striking a balance between the role of national sovereignty and shaping an equitable governance order.

Bibliography

1. Aaronson, Susan Ariel. "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review*, vol. 18, no. 4, 2019. https://doi.org/10.1017/S1474745618000198.

2. Abrhám, Josef, and Milan Vošta. "Impact of the COVID-19 Pandemic on EU Convergence." *Journal of Risk and Financial Management*, vol. 15, no. 9, 2022. https://doi.org/10.3390/jrfm15090384.

3. Annette Baier, *Trust and Antitrust*, 96 ETHIcs 231, 1986.

4. Barshefsky, Charlene. "EU Digital Protectionism Risks Damaging Ties with the US." *FT. Com*, 2020. https://www.proquest.com/docview/2476216082?parentSessionId=EqfmRdbS9T%2Fylvlqjhk4RWuXWbkCVi%2FXPL9OSvlxbTY%3D&pqorigsite=primo&accountid=14701&sourcetype=Trade%20Journals#center, Accessed: 25 Dec 2023.

5. Baylis, John, et al., editors. The Globalization of World Politics: An Introduction to International Relations. Eighth edition., *Oxford University Press*, 2020.

6. Bulletin of the European Communities, "Declaration on European Identity," Luxembourg: Office for official publications of the European Communities, 1973, No 12. https://www.cvce.eu/content/publication/1999/1/1/02798dc9-9c69-4b7d-b2c9f03a8db7da32/publishable_en.pdf.

7. Brown, Seyom. International Relations in A Changing Global System: Toward A Theory of The World Polity, Second Edition. Second edition., Taylor and Francis, 2018. https://doi.org/10.4324/9780429495168.

8. Carl Dahlman, et al. "Harnessing the Digital Economy for Developing Countries." *OECD Development Centre Working Papers*, Organization for Economic Co-Operation, and Development (OECD), 2016, https://doi.org/10.1787/4adffb24-en.

9. Csernatoni, Raluca. "The EU's Technological Power: Harnessing Future and Emerging Technologies for European Security." Peace, Security and Defence Cooperation in Post-Brexit Europe, Springer International Publishing, 2019, p. 119, https://doi.org/10.1007/978-3-030-12418-2_6.

10. Commission of the European Communities. European Governance: A White Paper, 2001.

11. Council of the EU. "Digital diplomacy: Council sets out priority actions for stronger EU action in global digital affairs", European Council, https://www.consilium.europa.eu/en/press/press-releases/2023/06/26/digital-diplomacy-council-sets-out-priority-actions-for-stronger-eu-action-in-global-digital-affairs/, Accessed: Dec 15, 2023.

12. Council of Europe, “Joint Statement on the right to data protection in the context of the COVID-19 pandemic”, https://rm.coe.int/covid19-joint-statement/16809e09f4, Accessed: 26 Jan 2024.

13. Council of Europe, “Convention on Cybercrime”, ETS 185-Cybercrime (Convention), 2001, https://rm.coe.int/1680081561, Accessed: 5 March 2024.

14. Council of Europe, “Strategy 2016-2019, Democracy, human rights and the rule of law in the digital world”, 2016, https://rm.coe.int/16806aafa9, Accessed: 6 March 2024.

15. Dear, Keith. “Beyond the ‘Geo’ in Geopolitics: The Digital Transformation of Power.” *The RUSI Journal*, vol. 166, no.7, 2021. https://doi.org/10.1080/03071847.2022.2049167.

16. Deutsch, Morton. “Trust and Suspicion”, *The Journal of Conflict Resolution*, Vol.2, No.4, 1958.

17. Durkalić, Danijela, et al. “The Measurement of Real Convergence in the EU-28 by Using the Entropy Method.” *Ekonomický Časopis*, vol. 67, no. 7, 2019.

18. European Commission. "Shaping Europe’s Digital Future." Digital Strategy, February 2022, https://digital-strategy.ec.europa.eu/en/policies/5g.

19. European Commission. “Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act), *Brussels*, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0767.

20. European Court of Human Rights. “Guide on Article 8 of the European Convention on Human Rights.” Publisher or Website, 31 August 2022, https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life.

21. European Commission, “A Digital Single Market for Europe，” 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192, Accessed: 10 Jan 2024.

22. European Commission. “Europe’s Digital Decade.” https://digital-strategy.ec.europa.eu/en/node/157/printable/pdf.

23. European Commission. “How contact tracing and warning apps helped during the COVID-19 pandemic”, https://commission.europa.eu/strategy-and-policy/coronavirus-response/travel-during-coronavirus-pandemic/contact-tracing-and-warning-apps-during-covid-19_en, Accessed: 25 Jan 2024.

24. European Commission. “2020 Mobile Contact Tracing Apps in EU Member States.” December 18, 2020.https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/trav-el-during-coronavirus-pandemic/mobile-contact-tracing-apps-eu-member-states_en. Accessed: 21 Jan 2024.

25. European Council, “GENERAL DATA PROTECTION REGULATION (GDPR) - Official Legal Text”, Article 9-2(j), https://gdpr-info.eu/art-9-gdpr/, Accessed: 25 Jan 2024.

26. European Data Protection Board. Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak. 2020 Apr 21. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf, Accessed: 25 Jan 2024.

27. European Data Protection Supervisor. “ANNUAL REPORT 2020”, European Union, 2021, https://edps.europa.eu/system/files/2021-04/2021-04-19-annual-report-2020_EN.pdf, Accessed: 16 Dec 2023.

28. European Union. “Aims and Values.” https://european-union.europa.eu/principles-countries-history/principles-and-values/aims-and-values_en, Accessed: 25 Jan 2024.

29. European Union. "Institutions: European Commission." https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission, Accessed: 12 Nov 2023.

30. European Union. “European Data Protection Supervisor (EDPS)”, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-supervisor-edps_en, Accessed, 18 Dec 2023.

31. European Union. “The European Data Protection Board (EDPB)”, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_en, Accessed, 18 Dec 2023.

32. European Union. “European Union Agency for Cybersecurity (ENISA)”, https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-union-agency-cybersecurity-enisa_en, Accessed, 18 Dec 2023.

33. Fligstein, Neil, et al. “European Integration, Nationalism and European Identity.” *Journal of Common Market Studies*, vol. 50, no. s1, 2012. https://doi.org/10.1111/j.1468-5965.2011.02230.x.

34. GDPR in 2020 and in the Future: Views from Brussels, Privacy Solved, https://privacysolved-com.translate.goog/gdpr-in-2020-and-in-the-future-views-from-brussels/?_x_tr_sl=en&_x_tr_tl=zh-CN&_x_tr_hl=zh-CN&_x_tr_pto=sc, Accessed: April 8, 2024.

35. Ghauri, Pervez, et al. “Research on International Business: The New Realities.” *International Business Review*, vol. 30, no. 2, 2021. https://doi.org/10.1016/j.ibusrev.2021.101794.

36. Harcourt, Alison. *Brexit and the Digital Single Market*. First edition., Oxford University Press, 2023, https://doi.org/10.1093/oso/9780192899378.001.0001.

37. Héritier, A., & Lehmkuhl, D. Governing in the Shadow of Hierarchy: New Modes of Governance in Regulation. In A. Héritier & M. Rhodes (Eds.), *New Modes of Governance in Europe: Governing in the Shadow of Hierarchy*. London, UK: Palgrave Macmillan, 2011.

38. Ingebrigtsen, Christine, and Susan Larson. "Interest and Identity: Finland, Norway and European Union." *Cooperation and Conflict*, vol. 32, no. 2, 1997, https://doi.org/10.1177/0010836797032002004.

39. Jia, Kai, and Nan Zhang. "Categorization and Eccentricity of AI Risks: A Comparative Study of the Global AI Guidelines." *Electronic Markets*, vol. 32, no. 1, 2022.

40. Jia, Kai, and Shaowei Chen. "Global Digital Governance: Paradigm Shift and an Analytical Framework." *Global Public Policy and Governance*, vol. 2, no. 3, 2022, p.286.

41. Jisen, Liu "EU ICT Industrial Policy and its Implications", *Party and Government Cadre Forum*, No. 6, 2007, p. 38.

42. Kaloudis, Martin. "Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan?" *New Global Studies,* vol. 16, no. 3, 2022. https://doi.org/10.1515/ngs-2021-0015.

43. Keohane, R. O., & Martin, L. L.," The promise of institutionalist theory", *International Security*, 1995, 20(1)

44. Kennedy, David (American law professor). "The Mystery of Global Governance." *Ohio Northern University Law Review*, vol. 34, no. 3, 2008.

45. Keohane, "Institutional Theory and the Realist Challenge after the Cold war," *Neorealism and Neoliberalism*, ed. by Baldwin.

46. Keohane, Robert O. *International Institutions and State Power: Essays in International Relations Theory*. 1st edition, Routledge, 2020.

47. Keohane, Robert O. (Robert Owen), and Joseph S. Nye. *Power and Interdependence*. 4th ed., Longman, 2012.

48. Keohane, Robert O. (Robert Owen). After Hegemony: Cooperation and Discord in the World Political Economy. *Princeton University Press*, 1984.

49. Leiter, Yechiel M. *John Locke's Political Philosophy and the Hebrew Bible.* Cambridge University Press, 2018.

50. Luhmann, Niklas, et al. *Trust and Power*. Wiley, 1979.

51. Morgenthau, Hans Joachim. *Politics among Nations*. 5th ed., Knopf., 1973, pp.118-121; Waltz, Kenneth Neal. *Theory of International Politics.* McGraw-Hill, 1979.

52. Na, Yang, and Hongyi, Chen. "Issue Spillover and Form Transformation: Understanding European Integration from the Dynamic Perspective", *European Studies*, Vol. 41, No. 2, 2023.

53. Nye, Joseph S. *The Regime Complex for Managing Global Cyber Activities.* CIGI, 2014, p.5.

54. Office for Official Publications of the European Communities. *Building the European Information Society for Us All*. 1997.

55. Oye, Kenneth A. *Cooperation under Anarchy*. Princeton University Press, 1986.

56. Partiti, Enrico. "TRUST AND GLOBAL GOVERNANCE: ENSURING TRUSTWORTHINESS OF TRANSNATIONAL PRIVATE REGULATORS." *New York University Journal of International Law & Politics*, vol. 52, no. 2, 2020.

57. Peggy Vissers, "Global Digital Compact: Deep Dive on Internet Governance", *UN New York*, 2023.

58. Peter, Fabienne, "Political Legitimacy", *The Stanford Encyclopedia of Philosophy* (Winter 2023 Edition).

59. Peterson, J., & Bomberg, E. (1999). *Decision-Making in the European Union.* London: Macmillan Press.

60. Raustiala, Kal, and David G. Victor. "The Regime Complex for Plant Genetic Resources." International Organization, vol. 58, no. 2, 2004. https://doi.org/10.1017/S0020818304582036.

61. Richter, Gesine, et al. "Patient Views on Research Use of Clinical Data without Consent: Legal, but Also Acceptable?" *European Journal of Human Genetics: EJHG*, vol. 27, no. 6, 2019, pp. 841–47, https://doi.org/10.1038/s41431-019-0340-6.

62. Roloff, Ralf. "COVID-19 and No One's World: What Impact for the European Union?" *Connections. The Quarterly Journal (English Ed.)*, vol. 19, no. 2, 2020. https://doi.org/10.11610/Connections.19.2.02.

63. Samusevych, Y.V., Novikov, V.V., Artyukhov, A.Ye., Vasylieva, T.A. (2021). "Convergence trends in the economy - education - digitalization - national security chain". *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, (6). https://doi.org/10.33271/nvngu/2021-6/177.

64. Sarah Collins-fattedad: "Towards a Global Digital Architecture", *CGA*, 2022, p.36.

65. Schneble, Christophe Olivier, et al. "Data Protection during the Coronavirus Crisis." EMBO Reports, vol. 21, no. 9, 2020. https://doi.org/10.15252/embr.202051362.

66. Seligman, Adam B. The Problem of Trust. Princeton University Press, 1997.

67. Shehaj, Albana. "How Is a European Identity Significant to the Future of the European Union?", Open Democracy (London), 2015, Retrieved from https://login.proxy.bib.uottawa.ca/login?url=https://www.proquest.com/magazines/how-is-european-identity-significant-future-union/docview/1684293873/se-2.

68. Simpson, J. A. (2007). Psychological Foundations of Trust. Current Directions in Psychological Science, 16(5). https://doi.org/10.1111/j.1467-8721.2007.00517.x.

69. Simmel, G. *The Sociology of Georg Simmel.* Transi., ed. and intr. by K. H. Wolff. New York: Free Press. 1950.

70. Strange, Susan. "Finance, Information and Power." *Review of International Studies*, vol. 16, no. 3, 1990, pp. 259–74, https://doi.org/10.1017/S0260210500112501.

71. Stuart, et al. "COVID-19: Putting the General Data Protection Regulation to the Test." *JMIR Public Health and Surveillance*, vol. 6, no. 2, 2020. https://doi.org/10.2196/19279.

72. Sztompka, Piotr. *Trust: A Sociological Theory*. Cambridge University Press, 1999

73. The Economist. "How technology is redrawing the boundaries of the firm", 2023. https://www.economist.com/business/2023/01/08/how-technology-is-redrawing-the-boundaries-of-the-firm. Accessed: March 1, 2024.

74. Thierry Chopin, "Europe and the identity challenge: who are we?", *Democracy and Citizenship*, 2018.

75. Tom R. Tyler, "Trust and Democratic Governance", *Trust and Governance*, 1998.

76. Triantafyllidis, Andreas, et al. "Features, Outcomes, and Challenges in Mobile Health Interventions for Patients Living with Chronic Diseases: A Review of Systematic Reviews." *International Journal of Medical Informatics (Shannon, Ireland)*, vol. 132, 2019. https://doi.org/10.1016/j.ijmedinf.2019.103984.

77. Voronkova, V., Punchenko, O., & Azhazha, M. "Globalization and global governance in the fourth industrial revolution (industry 4.0)". *Humanities Studies*, 2020, 182–200. https://doi.org/10.26661/ hst-2020-4-81-11.

78. Wiener, Antje, et al., editors. *European Integration Theory*. Third Edition., Oxford University Press, 2019.

79. Wolford, Ben. "What is GDPR, the EU's new data protection law?", *GDPR EU*, https://gdpr.eu/what-is-gdpr/. Accessed: 21 Jan 2024.

80. Yaqing, Qin. *Power, Institutions, and Culture*, 2nd edition, Peking University Press, 2016.

81. Zmerli, Sonja, and Tom W. G. van der Meer. “The Deeply Rooted Concern with Political Trust.” Handbook on Political Trust, Edward Elgar Publishing, 2017. https://doi.org/10.4337/9781782545118.00010.

82. Zygmuntowski, J. J. & Zoboli, L. & Nemitz, P. F. (2021). Embedding European values in data governance: a case for public data commons. Internet Policy Review, 10(3). https://doi.org/10.14763/2021.3.1572.