Acta Universitatis Danubius

JURIDICA

The General Data Protection Regulation of 2016 (GDPR) Meets its Sibling the Artificial Intelligence Act of 2024: A Power Couple, or a Clash of Titans?

Junaid Sattar Butt[1]

Abstract: The European Union (EU) Parliament and Council of the European Union adopted the General Data Protection Regulation of 2016 (**"the GDPR, 2016"**) (European Data Protection Supervisor, 2024) on 14 April 2016, to become effective on 25 May 2018 as an EU regulation (instead of a directive), GDPR is directly applicable with force of law on its own without the need of transposition and, widely considered one of the strictest data privacy and security laws globally while on March 13, 2024, the European Union (EU) Parliament adopted the world's first law governing "artificial inelegance" the EU Artificial Intelligence Act of 2024 (**"the AI Act, 2024"**)[2]. In the ever-evolving landscape of data governance and technological advancement, the intersection between the GDPR and the newly introduced AI Act, 2024 stands as a pivotal point of examination. While both regulations share the goal of protecting individuals' rights, their specific areas of focus and compliance requirements raise intriguing questions about their potential interplay. This research article explores the complex relationship between these two regulatory frameworks, exploring whether they function as a synergistic "power couple" or engage in a tumultuous "clash of titans". Through comprehensive analysis and critical evaluation, the article scrutinizes how the "power couple" of GDPR and the AI Act, 2024 function together, we aim to shed light on whether they will truly be a force for responsible AI development or lead to a "clash of titans" hindering innovation. Drawing upon legal, ethical, and practical perspectives, the study navigates through the complexities of data protection, algorithmic

[1] Master of Laws (LL.M), Postgraduate Institute of Law, the University of Lahore, Pakistan, Address: 1-Km Defence Road, near Bhuptian Chowk, Lahore, Punjab, Pakistan, Corresponding Author: junaidsattarbutt@yahoo.com ORCID Profile: https://orcid.org/0009-0000-0530-962X Researchgate Profile: https://www.researchgate.net/profile/Junaid-Butt-4.

[2] European Parliament. EU Artificial Intelligence Act, 2024. Retrieved April 26, 2024, from https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.

governance, and the ethical deployment of artificial intelligence. By elucidating the nuances of this regulatory interplay, the article contributes to a deeper understanding of the challenges and opportunities presented by the convergence of data protection and AI governance in the digital age. It will be of particular interest to researchers, policymakers, and businesses involved in the development and deployment of AI systems.

Keywords: GDPR and AI Act interplay; Balancing data protection and AI innovation; Responsible AI Development; Technological advancement; Data protection standards

1. Introduction

DAMA International defines Data Governance as "the exercise of authority and control (planning, monitoring and enforcement) over the management of data assets" (Earley, Henderson & Association, 2017). The General Data Protection Regulation of 2016 marked a significant milestone in global data protection law, introducing stringent measures to safeguard individual privacy rights in the digital age. However, the regulatory landscape has since evolved with the emergence of the Artificial Intelligence Act of 2024, a groundbreaking legislation addressing the governance of artificial intelligence (AI) systems within the European Union (EU). While both regulations aim to empower individuals and safeguard rights, a critical analysis is necessary. The GDPR's focus on data privacy and control might conflict with the AI Act's need for data access for certain AI applications. Conversely, the AI Act, 2024 emphasis on responsible development and risk management could reinforce the GDPR's objectives. This research explores the potential interplay between these regulations, examining how these regulations might work in synergy ("power couple") or create implementation challenges ("clash of titans"). Artificial intelligence (AI) has significantly impacted our daily lives, leading to concerns about data protection and ethics. The European Union (EU) has established itself as a leader in shaping the regulatory landscape for data privacy and artificial intelligence and developed regulations to ensure ethical AI development and data protection, including the GDPR, 2016[1], AI Liability Directive, 2022[2] and the AI Act, 2024. The

[1] European Parliament, Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[2] European Commission. (2022). Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM/2022/496 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

EU GDPR, 2016 ushered in a new era of data protection, empowering individuals with unprecedented control over their personal information. The EU embarked on its data governance journey with the groundbreaking GDPR, 2016, establishing a precedent for safeguarding personal data. Academic literature extensively delves into the GDPR's influence and the challenges in its implementation, critiquing consent-based models (Ruohonen & Mickelsson, 2023) and highlighting sphere transgressions by major tech firms (Sharon & Gellert, 2023). However, the GDPR, 2016 represented just the initial phase. Subsequent regulations such as the Digital Markets Act (DMA)[1], Digital Services Act (DSA)[2], Data Governance Act (DGA)[3], and the Data Act[4] have augmented the EU's data governance framework, with the EU AI Act, 2024 poised to further expand it. Each regulation targets different aspects of data governance, addressing the complexities of the digital economy. Studies have identified common values and approaches in the "Package Acts" (DMA, DSA, DGA) (Picht & Richter, 2022). Potential conflicts between the Data Act proposal and other regulations (Holznagel & Freese, 2023) have also been revealed. Furthermore, examination of the AI Act proposal has centered on the quest for "trustworthy AI," emphasizing trust as a pivotal factor in the data governance of AI technologies (Díaz-Rodríguez, et. al, 2023). In 2024, the arrival of the EU AI Act, 2024 marks a significant development, aiming to ensure the responsible development and use of AI technologies. The study Butt J**.** (Butt, 2024) analysis each and every corner of the World's First Artificial Intelligence (AI) Act, enacted in 2024, as a landmark development in regulating AI technologies. Focused on addressing AI challenges, the Act establishes clear guidelines, standards, and accountability mechanisms, prioritizing ethical considerations like fairness,

[1] European Parliament, Council of the European Union. (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925.

[2] European Parliament, Council of the European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

[3] European Parliament, Council of the European Union. (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/868/oj.

[4] European Parliament, Council of the European Union. (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/2854.

transparency, and privacy. Collaboration with various stakeholders is mandated, including governments, industry, academia, civil society, and the public. The Act's global impact is substantial, setting a precedent for other nations to develop their own AI regulations, potentially fostering greater harmonization of AI governance frameworks worldwide. To remain effective, the Act requires periodic reviews, amendments, and updates to adapt to advancing technologies and evolving societal expectations. Balancing innovation and regulation is pivotal, with the Act aiming to foster innovation while mitigating potential risks. Overall, the study underscores the importance of proactive and forward-thinking regulation in maximizing the benefits of AI technologies while safeguarding against potential harms, positioning the AI Act as a blueprint for responsible AI governance globally. As far as the rapidly evolving landscape of data governance and technological regulation, the convergence of the GDPR, 2016 and AI Act, 2024 represents a critical juncture. The EU However, these legal frameworks are not fully aligned, potentially creating challenges for users, AI system providers, and data subjects whose personal data is processed through these systems. This confluence of regulations presents a fascinating interplay and as these two regulatory giants intersect, questions arise regarding their compatibility, synergy, and potential conflicts. The GDPR of 2016 emphasis on strict data privacy controls might, at first glance, appear to be at odds with the AI Act of 2024 potential need for access to vast amounts of data to train and operate certain AI systems. Conversely, the AI Act's focus on responsible development, risk management, and bias mitigation could potentially reinforce the GDPR's objectives. The dissertation Antonaros V. (Antonaros, 2024) explores the intersection of AI systems and the GDPR, aiming to harmonize AI Law with data protection regulations for a comprehensive legal framework within the EU. It highlights the dual nature of AI as both beneficial and potentially infringing on personal data protection, emphasizing the need for alignment between AI Law and GDPR provisions to address these challenges effectively. This research delves into this complex dance between the GDPR, 2016 and the AI Act, 2024. We will explore areas of overlap, potential conflicts, and how organizations can navigate the combined demands of these regulations. By analyzing their interaction, we aim to shed light on whether these regulations will truly function as a "power couple" fostering responsible AI development, or if they might create a "clash of titans" that hinders innovation in the EU. Understanding this relationship is crucial for policymakers, researchers, and businesses alike as they navigate the evolving regulatory environment for AI and strive to build a future grounded in both innovation and ethical considerations.

2. Research Objectives

The study of the EU Artificial Intelligence Act, 2024 aims to analyze the legislative framework, evaluate its regulatory impact, compare it with existing AI regulations globally, understand stakeholder perspectives, identify compliance challenges, assess enforcement mechanisms, and explore implementation strategies. The Act's scope, goals, and implementation mechanisms will be analyzed, along with its potential socio-economic, technological, and ethical implications on stakeholders. Comparative analysis will be conducted to identify similarities and differences between the EU AI Act, 2024 and existing global regulations. Stakeholder perspectives will be explored, including policymakers, industry leaders, AI developers, and civil society. Compliance challenges will be identified, including data governance, transparency, accountability, and technical standards. Enforcement mechanisms will be assessed, including monitoring, enforcement actions, penalties, and cooperation among EU member states. Implementation strategies will be explored, including capacity-building measures, public awareness campaigns, and international collaboration on AI governance. Future developments will be predicted, and evidence-based policy recommendations will be provided to enhance the Act's effectiveness, fairness, and ethical alignment. This research will help scholars and policymakers gain insights into the implications and challenges of regulating AI technology, contributing to informed decision-making and responsible AI governance.

2.1. Research Question

Q: How do the General Data Protection Regulation of 2016 (GDPR) and the Artificial Intelligence Act of 2024 (AI Act) interact in terms of data protection and privacy rights within the context of AI technologies, and to what extent do they complement each other in regulating the ethical and responsible development and deployment of AI systems within the European Union? Additionally, what potential areas of conflict or tension exist between these regulations, and how might they be addressed to ensure coherence and consistency in AI regulation, while considering their impact on businesses, organizations, and individuals operating within the EU?

2.2. Research Design & Methodology

In crafting the research design for this study, the aim is to conduct a thorough investigation into the interplay between the General Data Protection Regulation (GDPR) of 2016 and its counterpart, the Artificial Intelligence Act (AI Act) of 2024, within the European Union (EU) context. The research design comprises several key elements to ensure a comprehensive analysis of this complex and evolving regulatory landscape. Firstly, the author undertakes a detailed review of existing literature, encompassing scholarly articles, government reports, legal documents, and industry publications, to establish a comprehensive understanding of the GDPR, 2016 and the AI Act, 2024 as well as their respective objectives, provisions, and implications for data protection, privacy rights, and AI regulation. Building upon this foundation, the author will employ a comparative approach to examine the extent to which the GDPR, 2016 and the AI Act, 2024 complement each other in regulating the ethical and responsible development and deployment of AI systems within the EU, while also identifying potential areas of conflict or tension between these regulations. To achieve this, the author also analyze the key provisions of both regulations, focusing on their alignment or divergence in areas such as data protection standards, transparency requirements, accountability mechanisms, and enforcement measures. Additionally, the author conduct interviews with relevant stakeholders, including policymakers, legal experts, industry representatives, and civil society organizations, to gather insights into their perspectives on the interaction between the GDPR, 2016 and the AI Act, 2024 and their implications for businesses, organizations, and individuals operating within the EU. Furthermore, the author utilize qualitative research methods, such as thematic analysis, to identify overarching themes and patterns emerging from the data, thereby contributing to a nuanced understanding of the dynamics between these two regulatory frameworks. Finally, the author will draw upon his findings to assess the broader implications of the GDPR, 2016 and the AI Act, 2024 for data protection, privacy rights, and AI regulation in the EU, and to offer recommendations for policymakers, businesses, and other stakeholders navigating this complex regulatory landscape. Through this comprehensive research design, the author aims to shed light on the nature of the relationship between the GDPR, 2016 and the AI Act, 2024 and to contribute to ongoing discussions surrounding the regulation of AI technologies within the EU.

3. Literature Review

The promulgation of the Artificial Intelligence (AI) Act, 2024 on 13th March, 2024 marks a significant milestone, while direct scholarly analysis of the EU AI Act, 2024 is limited in the immediate aftermath of its enactment; the broader literature on AI regulation and governance offers crucial context and insights into the implications of this groundbreaking legislation. The article is basically itself represent an analytical review of the original legislative text, however, by synthesizing existing research in this field, this review aims to provide a comprehensive understanding of the challenges, opportunities, and potential impacts associated with the EU AI Act, 2024 as well as avenues for future inquiry and exploration. The study Mlynář J. and Arminen I. (Mlynář & Arminen, 2023) emphasizes the significance of examining the obsolescence of social practices to understand social change and history. It suggests that ethno-methodology/conversation analysis (EM/CA) studies provide valuable insights into the transformation of social practices, particularly in the context of technological advancements and societal shifts. The study emphasizes the need for empirical investigation into obsolescence and persistence, and the integration of socio-historical perspectives into analytical frameworks. Overall, EM/CA studies are crucial in illuminating the historicity of human agency and social change. The study Kosurko et. al, (2023) (Kosurko, Arminen, Herron, Skinner & Stevanovic, 2021) examines the social connectedness of older adults living with dementia through a digitally delivered dance program, Sharing Dance Seniors. It compares digital vs. in-person interactions and uses an ethno-methodology and conversation analysis approach. The research aims to improve best practices and policy guidelines for digital program delivery and provide opportunities for older people and dementia residents to contribute to technology development. The systematic literature review Khakurel J. & Blomqvist K. (Khakurel & Blomqvist, 2022) provides insights into the integration of AI in teamwork settings, highlighting the need to balance opportunities and concerns. Factors such as design considerations, teammate interactions, task management, privacy, ethics, and machine teammates' behaviors must be addressed. By fostering collaboration among end-users, researchers, practitioners, and AI application developers, we can maximize AI's benefits while mitigating risks. Future research should focus on practical applications and real-world implications to harness AI's full potential in teamwork and collaborative productivity. The study Tero (Erkkilä, 2024) states that digitization in bureaucracies has led to improved service provision, responsiveness, participatory governance, and economic exploitation of public data. This has resulted in hybrid governance structures. However, contradictory trends, such as big data and algorithmic

governance technologies, have created new domains of information processing. This has led to a growing demand for control mechanisms to address citizen information rights and accountability. The study Gritsenko D. & Wood M. (Gritsenko & Wood, 2022) highlights the transformative effects of introducing algorithms into traditional governance modes, such as speeding, disinformation, and social sharing. Algorithmic systems influence rule development, communication dynamics, and relationship-building among governing actors. This leads to conflict resolution through pre-designed rules and decreased commitment. However, the degree of change varies across governance modes, with co-governance experiencing radical transformation. Further studies Hallamaa J. & Kalliokoski T. (Hallamaa & Kalliokoski, 2022) highlights that AI ethics can be improved by adopting a reality-based practice orientation, focusing on the actual consequences of AI's actions rather than high moral values. This approach encourages the discovery of practical solutions to ethical problems in AI design, ensuring that commercial interests align with ethical design. This approach makes AI ethics more accessible and contributes to practical morality. The studies Harju A. et. al. (2023) (Harju, Hallikas, Immonen & Lintukangas, 2023) reveals that procurement digitalization significantly enhances the resilience of Supply Chains (SCs) by improving information sharing, mediating the relationship between digitalization and resilience, and reducing uncertainty. This research is significant due to its novelty and lack of empirical research on its impact on SC disruption mitigation capabilities. Further studies Karttunen E. et. al. (Karttunen, Lintukangas & Hallikas, 2023) explores digital transformation of the PSM process, focusing on data infrastructure as the main intervention. Open standards and comprehensive data governance enable interoperability across functions and organizations. The study has limitations, such as a small sample size and not being applicable to small enterprises. Future research should investigate digital transformation in different sectors and technology- and application-centric discussions. The studies Wingström (Wingström, Hautala & Lundman, 2022) states that creativity in AI era should be redefined to co-creativity, focusing on the complex, spatial process between humans and AI, rather than human-centered creativity studies, as the future possibilities are endless. The Study Vangard Littler (2024) (Littler, 2024) highlights that the EU Parliament has adopted the AI Act, 2024 a significant milestone in AI regulation, with a majority vote. The Act categorizes AI systems into risk tiers, triggering different regulatory consequences. High-risk systems face bans and market withdrawal, while transparency obligations apply to all systems. The study Schutte S. B.et. al. (Schutte, Majewski & Havu, 2021) examines damages liability for AI-related harm in the EU, highlighting the need for

novel EU rules. The Commission White Paper aims to use AI for society and economy while addressing moral and legal issues. The paper Byanjankar et al. (Byanjankar, Mezei & Heikkilä, 2021) proposes a data-driven model for P2P lending decision-making, identifying an optimal portfolio of loans using an instance-based credit-risk assessment framework. The model uses the expected-value framework and kernel estimations, offering better performance than existing models. The study Stark et. al. (Stark, et. al, 2023) states while the digitalization of manufacturing at Väderstad is still ongoing, the way in which the company has digitalized reveals what can be achieved and how, presenting an operations strategy that other original equipment manufacturers can follow. The study Kuypers L. (Kuypers, 2024) states the EU design law lacks a solid foundation for AI-driven designs, making it unclear whether they can be protected under design law. This leaves a need for a more comprehensive legal framework to protect both creators and intellectual property rights holders while encouraging AI use in the design process. Designers should be aware of the legal implications and risks associated with AI-programs, verifying data sources, and reviewing AI program terms and conditions. The European Union Parliament recently adopted the "Artificial Intelligence Act, 2024" the first legal framework on AI, to provide clear requirements and obligations for AI developers, deployers, and users. The Act prohibits AI systems with unacceptable risks from being deployed in the EU and regulates the deployment of foundation models, including compliance with copyright law and technical documentation. Eric Leikin et. al. (Leikin, Riede, Hofer & Sue, 2024) highlights the significant impact of technology on various sectors, including increased risk of disputes. The study Susarla (Susarla, 2024) highlights the use of Generative AI tools like ChatGPT, which are based on foundational models trained on vast amounts of data. These models use machine learning methods to understand data relationships, mimicking cognition and reasoning. However, the widespread use of generative AI raises concerns about intellectual property and copyright protection. Researchers argue that AI trained on copyrighted works is not an infringement, but audit studies show that end users can produce works that resemble copyright-protected content. Researchers suggest methods to make AI models unlearn copyrighted data, such as red teaming or reducing similarity between outputs and copyrighted material. The study Katharine Miller (Miller, 2024) shows AI models using Google Street View images can identify visual indicators of gentrification, enabling early identification and intervention. This accuracy demonstrates the potential of interdisciplinary approaches and innovative datasets to address complex societal issues, enabling targeted interventions for vulnerable communities and equitable urban development.

The study Yigit Y. et. al. (Yigit, Buchanan, Tehrani & Maglaras, 2024) explores the use of Generative Artificial Intelligence (GenAI) in cybersecurity, highlighting its potential to automate defenses, enhance threat intelligence, and improve protocols. However, it also highlights the need for robust ethical, legal, and technical scrutiny to minimize data misuse risks and maximize the benefits of GenAI in protecting digital infrastructures. Future research should focus on creating strong ethical standards and creative defense mechanisms to handle GenAI challenges and ensure fair implementation. A multidisciplinary effort is needed to balance GenAI's innovative capabilities with cybersecurity resilience. A Study Butt (Butt, 2023) explores the use of Artificial Intelligence in administrative decision-making is a complex issue requiring ethical and legal considerations. While it offers benefits like improved efficiency and cost savings, it also poses risks. Comparative studies can inform policymaking, ensuring transparency, accountability, and respect for privacy and human rights. AI adoption is expected to significantly impact labor markets, with cross-country differences and uncertain implications. The research Oinas S. & Hotulainen R. (Oinas & Hotulainen, 2022) highlights the varying preferences among students regarding the use of digital tools versus traditional pen and paper methods, particularly in tasks such as searching for answers, writing syntheses, and assessing the reliability of information. The study Kalliokoski (Kalliokoski, 2023) explores the integration of technology in modern society, emphasizing its practical benefits and societal changes. It emphasizes the importance of human cooperation, creativity, and theological perspectives in understanding and engaging with smart technologies. The study Nguyen Q.M. et. al. (Nguyen, Tran, Kanniainen, Iosifidis & Gabbouj, 2023) focuses on creating an algorithm using neural networks to optimize investment strategies in the cryptocurrency market. It aims to construct portfolios using derivative assets from cryptocurrency brokers, using a deep neural network to determine asset allocation weights. Further studies Gkritsi, E. (Gkritsi, 2024) states that the AI Act, 2024 unlike the GDPR, doesn't regulate every use of AI or follow long precedents. It's a mix of fundamental rights, product safety, liability, and digital safety. The impact on European startups is debated, as European AI companies attract less capital than US or Chinese counterparts. Implementing the law quickly and effectively is crucial for obtaining legal certainty. Human rights groups (Hakobyan, 2024) have raised concerns that the law doesn't go far enough in protecting individuals (Cabrera, 2024), particularly biometrics use and AI within an immigration context, such as identity checks. In the study Sjödin D. et. al. (Sjödin, Liljeborg & Mutter, 2024) importance of ecosystems and platforms in AI-enabled CBMs is highlighted, and further studies could investigate the linkages between

industrial digital platforms, AI, and circularity. The study Koivisto I. (Koivisto, 2023) discuss that Finland's parliament has passed legislation enabling automated decision-making in public administration, despite ongoing debates on balancing automation efficiency with legal principles and citizen protections. The new law requires routine, non-discretionary decisions and citizen notification in case of errors. This marks a significant shift towards automation in Finnish public administration. The study Rantanen & Komp-Leukkunen (Rantanen & Komp-Leukkunen, 2023) explores the impact of digitalization on self-employed older adults, finding both challenges and opportunities. Entrepreneurs face the challenge of adapting to new technologies, while retirement planning is influenced by their routines. Another study Korpisaari (Korpisaari (ex. Tiilikka), 2022) finds that the internet has transformed information dissemination, blurring the lines between traditional journalism and other forms of communication. Artificial intelligence can create content without human involvement, raising legal questions, especially around the EU's General Data Protection Regulation (GDPR). The study Butt (Butt, 2023) explores regulatory approaches to digital currencies and the role of International Financial Institutions (IFIs) in fostering global cooperation for harmonized accounting standards. The study Sankari S. et. al. (Sankari, Koulu, Hirvonen & Heikkinen, 2023) explores the relationship between law, technology, and society, focusing on the definition dilemma related to AI and the EU Commission's Artificial Intelligence Act (AIA). It highlights the long-standing relationship between law, technology, and society, suggesting a critical take on the AI definition dilemma and the regulation of AI. Research Studies James Landay et. al. (Lynch, 2024) at World Economic Forum in Davos, Switzerland highlighted the impact of AI on work dynamics, business strategies, and productivity. Key speakers discussed the need for active implementation, addressing AI risks, and promoting a human-centered approach. Further Studies Viljanen M. & Parviainen H. (Viljanen & Parviainen, 2022) explores the heuristic stratigraphy of AI-related law presents a complex, fragmented set of rules with diverse scopes and targets. Five key themes include the need for detailed rules, uneven regulatory layers, rule scopes, regulatory instrument types, and the unsettled nature of AI law, which will likely persist in the future. A study Bauroth M. et. al. (Bauroth, Rath-Manakidis, Langholf, Wiskott & Glasmachers, 2024) proposes a maturity model for Human-Centered AI (HCAI), aiming to support AI development practices in companies, ensuring efficient, trustworthy, and safe AI solutions, considering fairness, transparency, accountability, and ethics. The chapter Cowley B.U. et. al. (Cowley, Charles, Pfuhl & Rusanen, 2023) presents a thought experiment using an MMOG simulation to

study AI deployment solutions in AIEd, focusing on explainable AI and Rawlsian distributive justice. The AIEd-MMOG meets all ART principles, including accountability, responsibility, and transparency and the simulation facilitates reproducible AI and supports XAI for more transparent, interpretable, and ethical AIEd. The study Laukkanen T. et. al. (Laukkanen, et. al, 2021) explores the potential of virtual technologies in promoting sustainable consumption by reducing travel time and enhancing various aspects of human life, such as leisure, work, and shopping. As VR devices become more user-friendly, they can significantly impact sustainable consumption decisions and green choices. The study van Gerven M. (van Gerven, 2022) reveals that algorithmic management positively impacts the meaningfulness of work through identity and belonging, while algorithmic control negatively affects it. It also reveals that algorithmic matching indirectly influences work meaningfulness, and it both facilitates and restricts crowd worker identity formation. The study Parkatti A. et. al. (Parkatti, Saari, Tammelin & Villi, 2022) identify three main frames of digital competence (DC) in media work: individual attitude, team-level support, and organizational-level practice. The individual attitude frame emphasizes employees' attitudes towards DC, the team-level support frame emphasizes the need for support within the work community. The study Mäkelä E. et. al. (Mäkelä, et. al, 2020) discuss the challenges faced by Digital humanities and social sciences projects due to data complexity and gaps between their objectives and computational means. It suggests that interactional support, integrating statistical analyses with qualitative judgement, and open science can improve research reliability and quality. However, it emphasizes the need for more value in the unseen work involved in data transformation. The study Toset S. et. al. (Toset, Late & Kumpulainen, 2023) highlights the complexity of creating an infrastructure for digital humanities and computational social sciences, highlighting the diverse information needs of users. Disciplinal differences between social sciences, humanities scholars, and computer and data scientists may impact the development of such infrastructure. This paper Collan M. (Collan, Savolainen, Virolainen & Luukka, 2023) presents a vision for a highly automated digital urban manufacturing network, focusing on decentralized micro-production and a central market mechanism for matching designers, customers, and producers. It discusses benefits and practical implications. The study Lamberg J.-A. et. al. (Lamberg & Luoma, 2021) explores vicarious learning-related communication practices in organizations, identifying two logics: predevelopment and procession and highlights the impact of ideology on communication and learning outcomes. Another study Premathilake G. W. et. al. (Premathilake, Li, Liu & Helander, 2021) explores the growing interest in

Artificial Intelligence (AI) robots in Information Systems (IS) domain, highlighting the fragmented literature and lack of comprehensive understanding of current service robot research. The article Davoodi L. & Meze J. (Davoodi & Mezei, 2022) compares machine learning models and language transformer models for sentiment analysis in e-commerce platforms. It finds neural network-based models offer higher accuracy in sentiment classification tasks. Manual annotation helps avoid issues with user ratings. Future research should focus on aspect-based sentiment classification to understand sentiment polarity and improve customer satisfaction. Limitations include representative sample, incorrect sentiment assignments, and availability of multiple machine learning models. The chapter Pihlajarinne T. & Alen-Savikko A. (Pihlajarinne & Alen-Savikko, 2022) emphasizes the need for rethinking AI concepts and creating context-specific solutions for the media sector. It suggests improving AI knowledge, acknowledging human involvement, and promoting balanced data availability. It also emphasizes human control and not overestimating AI's impact on social issues. Further studies Asatiani A. et. al. (Asatiani, Copeland & Penttinen, 2023) emphasizes the importance of compatibility between the chosen deployment model and RPA technology, considering the organization's existing systems and capabilities, and the sourcing model and RPA technology. It recommends balancing internal and external resources, focusing on long-term development, and retaining competent staff. Organizations must also assess their objectives and adjust their deployment strategy as technology evolves. The study Nikunen K. (Nikunen, 2023) explores the impact of digitalization on self-employed older adults, finding both challenges and opportunities. Entrepreneurs must adapt to new technologies, which can be challenging due to frequent updates and client demands. Digitalization can also influence retirement planning, with some avoiding new technologies and others focusing on routines. Further research is needed to understand other self-employed workers' experiences. The study Nadeem et. al. (Nadeem, Ali, Rehman & Saarinen, 2023) identifies barriers to digitalization in Pakistan's economy, including inadequate ICT infrastructure, lack of business awareness, and market challenges, using ISM and QFD. It recommends AI, machine learning, advanced analytics, research, and standardization of digital processes as effective measures. The study Siitonen M. et. al. (Siitonen, Laajalahti & Venäläinen, 2024) explored include testing and developing algorithmic tools, developing practices and policies for journalistic work, attitudes and technology acceptance, and societal and macro-level discourses concerning AI and journalism. The study van Zoonen W. et. al. (van Zoonen & Treem, 2024) examines the impact of algorithmic management on the perceived meaningfulness of work among crowd workers. The EU AI Act, 2024, has been

analyzed in relation to social practices, digitalization, and technological advancements. The review highlights the importance of understanding social change through ethno-methodology/conversation analysis and the transformative effects of algorithms on traditional governance modes. It also discusses the ethical implications of AI, proposing reality-based practice orientations for improvement. The review also highlights the legal implications of AI-driven designs, emphasizing the need for comprehensive legal frameworks to protect intellectual property rights. It also highlights AI's role in identifying visual indicators of gentrification and enhancing cybersecurity, emphasizing the need for ethical standards and robust defense mechanisms. The study Weinhardt C. et. al. (Christof, Jonas, Hinz & Wil, 2024) focuses on the impact of digital authoritarianism on democratic institutions and the role of Information Systems in understanding and addressing this phenomenon. It likely involves analyzing digital platforms and ecosystems within authoritarian states to assess their influence on democratic processes. Additionally, it may explore strategies for utilizing technology to strengthen democratic structures in the face of digital transformation and geopolitical challenges. The study Polyzou F. (Polyzou, 2024) underscores the challenge of balancing AI innovation and data privacy under the AI Act and GDPR, especially concerning data minimization, transparency, and anonymization. Policymakers must prioritize interdisciplinary collaboration and a flexible regulatory approach to ensure alignment with evolving technology and societal needs while mitigating risks through carefully designed regulatory sandboxes. This study Fresz B. et. al. (Fresz, Dubovitskaya, Brajovic, Huber & Horz, 2024) examines the intersection of law and explainable Artificial Intelligence (XAI), particularly focusing on European and German law alongside international regulations like GDPR. It derives XAI-method requirements from legal bases, revealing varied needs for XAI properties across different laws, suggesting current XAI methods lack full satisfaction, particularly in correctness and confidence estimation. This study Khalfa R. et. al**.** (Khalfa, Theinert & Hardyns, 2024) explores the impact of big data policing within the EU context, regulated by laws like GDPR and the forthcoming AI Act. It emphasizes the need for effective oversight, particularly focusing on decision-makers' agency and the integration of human-centric design principles, proposing a framework to enhance ethical practices in the application of big data policing, specifically in spatiotemporal crime prediction. The paper Zuiderveen B. et. al. (Borgesius, Hacker, Baranowska & Fabris, 2024) offers a beginner-friendly overview of non-discrimination law in Europe, tailored for computer scientists and AI users. It emphasizes the unique aspects of European non-discrimination law, covers EU-wide rules, distinctions between direct and indirect

discrimination, and explores relevant cases from GDPR and the EU AI Act, with additional reading suggestions provided. The study Duflot A. (Duflot, 2024) discusses the potential for AI to replace judges in legal processes, citing examples from foreign experiments where software is used to settle disputes, highlighting benefits like reduced court congestion. However, concerns about ethical issues such as algorithmic opacity and biases persist, urging legal professionals to adapt while ensuring ethical compliance. Key future considerations for AI in justice include legal certainty, compensation for algorithmic damages, and the balance of judicial control amidst the development of regulatory frameworks. The study Bruno P. (Peeters, 2024) examines the use of AI systems in EU tax administrations, highlighting concerns about the protection of taxpayers' rights and the need for human control during the tax collection process. While the GDPR allows for exceptions to purely automated decisions in tax matters, explicit guidance on protecting individuals' rights is lacking, necessitating clearer regulation, especially as AI's role in tax collection evolves. This chapter Zanfir-Fortuna G. (Zanfir-Fortuna, 2024) underscores the centrality of data protection law within the EU's Digital Rulebook, highlighting its application across various new laws and frameworks. It emphasizes the role of the GDPR as a common denominator in regulating the processing of personal data and identifies challenges in enforcement, suggesting coherent policymaking and governance to address them effectively. The study Wolff J. et. al. (2024) (Wolff, Lehr & Yoo, 2023) emphases that regulators in the EU and other countries are grappling with AI policy frameworks, evident in the EU's creation of new regulatory categories but minimal alterations in provisions. This highlights a struggle to address diverse AI risks, possibly leading to a reliance on GDPR rather than the AI Act for enforcement, potentially rendering the latter symbolic rather than actively enforceable. The study G'sell F. (G'sell, 2024) highlights that AI Liability Directive focuses on high-risk AI systems, aiming for targeted harmonization without overhauling national liability frameworks. Its alignment with the AI Act suggests future iterations may encompass provisions for GPAI models and generative AI, although progress is currently halted. Zanfir-Fortuna G. (Zanfir-Fortuna, 2024) analysis examines the interplay between EU data protection law, including Article 8 of the EU Charter and the General Data Protection Regulation, and the EU's new digital rulebook introduced in 2020. It argues that despite the complexity of new digital regulations, data protection law and its enforcement agencies remain central in safeguarding fundamental rights and mitigating risks associated with personal data processing in the digital realm. Bratu I. & Leiser M. (Bratu & Leiser, 2024) explores the evolving landscape of Cyberlaw and its

legislative milestones, including groundbreaking regulations such as the GDPR, DMA, and DSA, alongside national measures like the UK's Online Safety Bill and Germany's NetzDg, reflecting a pivotal phase in legal responses to digital transformation. The paper Romero-Moreno (Romero-Moreno, 2024) critiques the EU AI Act's deepfake provisions for potentially infringing on privacy and freedom of expression rights, proposing procedural safeguards for compliance. It highlights ambiguities in the Act's high-risk label, platform responsibilities, tracking methods, and data sharing, urging clear definitions, transparent oversight, and robust safeguards to prevent misuse and protect individual rights. The study Vellinga N. E. (Vellinga, 2024) explores the potential of a compensation fund to reconcile damages from AI systems with innovation, examining existing legal frameworks and proposing a design aligned with the EU's AI Act. It suggests such a fund could ensure fair compensation for personal and mental injuries, fostering innovation while addressing liability risks and promoting societal acceptance of high-risk AI systems. The study Weismann (Weismann, 2024) emphases that absence of international treaties governing nation-state relations in cyberspace stems from challenges such as fragmentation, interoperability, and localization, compounded by treaty harmonization issues and mistrust between nations. Proposed roadmaps advocate for collective action, multilateral cooperation, and consideration of human rights and privacy concerns to address cybercrime and insecurity, emphasizing the necessity of a collective response across sectors. Stockman, C. et. al. (Stockman, O'Connell, & Nottingham, 2024) highlights that cute design, while powerful and psychologically impactful, can also serve as a potential dark pattern, concealing manipulative tactics within digital technologies. Despite its widespread use and appeal, especially in software targeting children, there's a need for increased awareness and regulation to mitigate the risks associated with cute design's potential to enhance consumer manipulation. Bratu I. & Leiser M. (Bratu & Leiser, 2024) highlights the significance of the curate articles from the BILETA Conference 2023, discussing pivotal legislative milestones in Cyberlaw and their implications for legal frameworks in the digital age. It emphasizes the need for robust, adaptable, and equitable legal frameworks to address the complexities and challenges of technology in society. Kalsi M. (2024) (Kalsi, 2024) states that the analysis of DPAs' decisions regarding Article 25 GDPR reveals the importance of controllers' responsibility for compliance, especially concerning their relationships with processors. DPAs emphasize the necessity for controllers to have absolute control over their processors and to ensure that appropriate technical and organizational measures are implemented, as demonstrated in various enforcement actions. Tools such as audits,

contracts, and codes of conduct play a crucial role in operationalizing this leverage, facilitating compliance throughout data value chains and enhancing the effectiveness of DPbDD. The study Kruse N. et. al. (Kruse, Wachter & Schöning, 2024) suggests that the integration of artificial intelligence (AI) into agriculture faces challenges in legal compliance, particularly with emerging regulations like the EU AI Act and GDPR. To address this, a support app is being developed to simplify legal aspects, promoting compliance and awareness among developers and facilitating the seamless integration of AI into agriculture, aligning with evolving regulations. The study Pathak M. (Pathak, 2024) shows that evolution of EU Data Regulations from the GDPR to the AI Act, 2024 signifies a broadened scope and inclusivity in regulating data across various entities, reflecting the EU's ambition to foster a unified data market and encourage collaborative data practices. Despite imposing additional obligations, the framework aims to balance fundamental rights protection, innovation promotion, and the creation of fair and competitive digital markets in the digital era. The study Green D. (Green, 2024) highlights how policy drafting employs indeterminacy and its impact on informed consent compliance with the GDPR. Findings reveal prevalent use of indeterminacy in privacy policies, complicating understanding, and suggesting a need for clearer language and education initiatives to empower data subjects for informed decision-making in privacy matters. The study Mesinovic M. (Mesinovic, 2024) states that explainability in automated decision-making (ADM) systems provides transparency for developers and users to detect flaws and biases, fostering trust. Despite technical and legal hurdles, progress frameworks aim to ensure reliability in ADM applications, crucial for upholding standards and preventing rights violations. In conclusion, the literature review provides a comprehensive understanding of the regulatory landscape surrounding artificial intelligence (AI), particularly in the context of the General Data Protection Regulation (GDPR) and the Artificial Intelligence Act of 2024. Through synthesizing existing research, this review illuminates the challenges, opportunities, and potential impacts associated with the EU AI Act, offering insights into future inquiries and explorations. The review underscores the importance of interdisciplinary collaboration, ethical considerations, and adaptable regulatory frameworks to ensure responsible AI development and adoption while safeguarding fundamental rights and societal values. By integrating insights from various studies, this review contributes to a deeper understanding of the complex interplay between law, technology, and society in the digital age, paving the way for informed policymaking and regulatory action.

4. Case Laws

The Court of Justice of the European Union (CJEU) issued several significant data protection rulings in 2023, elucidating various aspects of the General Data Protection Regulation (GDPR). Among the key inquiries addressed by the court are the transparency requirements regarding data-sharing, the grounds for exercising the right to erasure, the types of damages applicable in legal claims, the grounds for making subject access requests, and the liability for administrative fines under the GDPR. In the case of "Österreichische Post" (C-154/21, January 12, 2023)[1], the court deliberated on the obligation of controllers to inform data subjects about the recipients or categories of recipients of their personal data. The ruling specified that controllers must disclose the specific organizations receiving personal data, except when it is genuinely impossible to do so. Moreover, in the case of "UZ v Germany" (C-60/22, May 4, 2023)[2], the court clarified that the right to erasure applies only when personal data have been unlawfully processed, distinct from violations of the accountability principle. Consequently, the absence of a Record of Processing Activities (RoPA) does not automatically warrant erasure if a valid legal basis for processing exists. In "Österreichische Post" (C-300/21, October 6, 2023)[3], the court addressed the types of damages claimable in private GDPR legal actions, emphasizing that punitive damages are not applicable. Instead, courts may award material and non-material damages, without punitive intentions, to compensate data subjects for harm suffered. Furthermore, in "FT v DW" (C‑307/22, October 26, 2023)[4], the court discussed the grounds for making subject access requests,

[1] Court of Justice of the European Union. (2023, January 12). Judgment of the Court (First Chamber) of 12 January 2023. RW v Österreichische Post AG. Request for a preliminary ruling from the Oberster Gerichtshof. Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject's right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions. Case C-154/21. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0154.

[2] Court of Justice of the European Union. (2023, May 4). Judgment of the Court (Fifth Chamber). In Case C-60/22. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4850182.

[3] Court of Justice of the European Union. (2023, May 4). Judgment of the Court (Third Chamber). In Case C-300/21. Retrieved from https://eu.vlex.com/vid/ui-contro-osterreichische-post-930388280.

[4] Court of Justice of the European Union. (2023, October 23). Reference for a preliminary ruling – Processing of personal data – Regulation (EU) 2016/679 – Articles 12, 15 and 23 – Data subject's right of access to his or her data undergoing processing – Right to obtain a first copy of those data free of charge – Processing of a patient's data by his or her medical practitioner – Medical records – Reasons for the request for access – Use of data for the purpose of triggering the liability of the person providing treatment – Concept of 'copy'. In Case C‑ 307/22, REQUEST for a preliminary ruling under Article

emphasizing that individuals can request access to their personal data for reasons beyond verifying lawfulness. Additionally, individuals are entitled to receive a full copy or a faithful and intelligible summary of their personal data upon request. In case "Deutsche Wohnen" (C-807/21) and "NVSC" (C-683/21, December 5, 2023)[1], the court clarified that liability for administrative fines under the GDPR requires intentional or negligent conduct, not strict liability. Additionally, processors may be held liable for damages if they process personal data against the controller's instructions for their own purposes. In the case of VB v Natsionalna agentsia za prihotide (Case C-340/21)[2], the Court of Justice of the European Union (CJEU) addressed a cyberattack on the Bulgarian tax authority (NAP), resulting in the unauthorized disclosure of personal data. The CJEU concluded that individuals may have suffered "non-material damage"—and therefore be able to claim compensation—if they can demonstrate that they feared future misuse of personal data that was compromised in a personal data breach. In the case of VX and AT v Gemeinde Ummendorf (Case C-456/22)[3], the CJEU addressed compensation for non-material damage resulting from the unauthorized publication of personal data. The CJEU clarified that Article 82 GDPR does not require a de minimis threshold of damage, and compensation should be awarded based on the actual harm suffered, without imposing a minimum level of harm. In case Krankenversicherung Nordrhein (Case C-667/21) (Matheson, 2024), the CJEU confirmed that compensation under Article 82 GDPR is compensatory rather than punitive. The burden of proof lies with the controller to demonstrate compliance with GDPR obligations and absence of responsibility for the damage. These judgments underscore the importance of robust

267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 29 March 2022, received at the Court on 10 May 2022, in the proceedings. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3588036.

[1] Court of Justice of the European Union. (2023, December 5). Judgments in Cases C-683/21 and C-807/21. Retrieved from https://www.debandt.eu/fr/node/665

[2] Court of Justice of the European Union. (2021). Case C-340/21: Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021 — VB v Natsionalna agentsia za prihodite. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0340.

[3] Court of Justice of the European Union. (2022). Judgment of the Court (Third Chamber) of 14 December 2023. VX and AT v Gemeinde Ummendorf. Request for a preliminary ruling from the Landgericht Ravensburg. Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 82 – Right to compensation and liability – Concept of 'non-material damage' – Online publication of the agenda for a municipal council meeting containing personal data – Publication without the consent of the data subjects – Claim of those data subjects seeking compensation for non-material damage. Case C-456/22. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0456.

security measures and prompt data breach response procedures to mitigate risks and potential compensation claims under the GDPR. The Court of Justice of the European Union (CJEU) issued a pivotal judgment on March 7, 2024, in the Endemol Shine case (Case C‑740/22)[1], clarifying the interaction between personal data protection and public access to documents under the EU General Data Protection Regulation (GDPR). Originating from Endemol Shine's oral request to a Finnish District Court for information on criminal proceedings related to one of its competitions, the case involved the District Court's refusal to orally disclose the information due to a perceived lack of legal basis. Endemol Shine appealed to the Court of Appeal – Eastern Finland, prompting the CJEU to address whether oral transfer of personal data constitutes data processing and if data on criminal convictions can be orally disclosed for public access. In its ruling, the CJEU broadly interpreted the concept of "processing" under the GDPR to include oral disclosure of personal data, aligning with the regulation's goal of robust data protection. It emphasized that allowing oral disclosure to evade GDPR provisions would contradict its fundamental purpose. Additionally, the CJEU determined that oral disclosure of personal data, particularly data related to criminal convictions stored in a court's register, constitutes processing under the GDPR, unless it involves manual processing without a filing system, which was not applicable in this case. Concerning the interplay between the GDPR and public access to official documents, especially regarding sensitive data like criminal convictions, the CJEU emphasized the necessity of striking a balance between access rights and data protection. It concluded that unrestricted disclosure of such information to any requester, without the demonstration of a specific interest, would violate the GDPR's provisions due to its potential infringement on fundamental rights. In case BL v MediaMarktSaturn (C-687-21), the CJEU restated its existing case-law, and expanded upon its analysis in VB by clarifying that alleged harms cannot be "purely hypothetical". In case Kočner v Europol (C-755/21), the CJEU awarded non-material damages of €2000 for the publication in newspapers of transcripts of "intimate" text messages. In GP v Juris GmbH (C-741/21), the CJEU found that where one processing activity

[1] Court of Justice of the European Union. (2024, March 7). JUDGMENT OF THE COURT (Sixth Chamber). Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Articles 2, 4, 6, 10 and 86 – Data held by a court relating to the criminal convictions of a natural person – Oral disclosure of such data to a commercial company on account of a competition organised by that company – Concept of 'processing of personal data' – National legislation governing access to those data – Reconciliation between the right of public access to official documents and the protection of personal data. https://curia.europa.eu/juris/document/document.jsf?text=&docid=283530&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

infringes multiple provisions of the GDPR, this should not allow claimants to "double-count" the harm they suffered. In conclusion, the rulings by the Court of Justice of the European Union (CJEU) in 2023 and 2024 significantly shape the interpretation and application of the General Data Protection Regulation (GDPR) within the European Union (EU). These rulings address crucial aspects such as transparency requirements, grounds for exercising rights, types of damages, liability for administrative fines, and compensation for non-material damage resulting from data breaches or unauthorized disclosure. Notably, the CJEU's broad interpretation of "processing" under the GDPR emphasizes the importance of robust data protection measures, while also highlighting the need to balance access rights with data protection principles. Moreover, the CJEU's emphasis on awarding compensatory rather than punitive damages underscores the GDPR's goal of providing redress to individuals affected by data protection violations. These judgments underscore the evolving regulatory landscape and the ongoing efforts to reconcile the principles of data protection with the demands of public access and accountability.

5. Historical Foundations

In examining the historical foundations of the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024, we delve into the legislative evolution that has shaped the regulatory landscape governing data protection and artificial intelligence (AI) within the European Union (EU). The GDPR, enacted in 2016, emerged as a response to growing concerns over data privacy and security in an increasingly digitalized world. Rooted in principles of transparency, accountability, and individual rights, the GDPR sought to modernize and harmonize data protection laws across the EU, establishing a comprehensive framework for the collection, processing, and storage of personal data. Conversely, the AI Act of 2024 represents a more recent development, reflecting the EU's evolving approach to regulating emerging technologies like AI. With a focus on ethical AI practices, human oversight, and risk management, the AI Act aims to address the challenges and opportunities posed by AI while ensuring alignment with societal values and human rights. By tracing the historical foundations of these two landmark legislations, we gain insights into the trajectories of data protection and AI regulation within the EU, setting the stage for an exploration of their intersecting paths and potential synergies or conflicts.

5.1. Historical Foundation of the GDPR, 2016

The journey of the General Data Protection Regulation (GDPR), 2016 began with the realization that advancements in technology necessitated a review of existing data protection laws. In 2016, the European Union (EU) replaced the outdated 1995 Data Protection Directive with the GDPR, marking a significant milestone in data protection legislation. Member States were given a two-year window to ensure full implementation of the GDPR by May 2018. The timeline of events leading to the adoption of the GDPR is marked by key milestones and deliberations. It started with the European Data Protection Supervisor's opinion on the European Commission's Communication in 2011, followed by the proposal for a comprehensive reform of data protection rules by the European Commission in 2012. Over the years, various opinions and updates from the European Data Protection Supervisor and the Article 29 Working Party contributed to the evolution of the GDPR. One of the GDPR's notable features is its expanded territorial reach, requiring organizations outside the EU to comply with its regulations when offering goods or services to EU residents. Additionally, the GDPR introduced the accountability principle, emphasizing the need for organizations to demonstrate compliance with data protection principles. The adoption of the GDPR by the European Parliament in 2014 and the subsequent agreement reached between the Parliament, the Council, and the Commission in 2015 paved the way for its formal enactment. The GDPR entered into force in 2016, with provisions aimed at reinforcing existing data protection rights and establishing new ones for individuals. On May 25, 2018, the GDPR officially came into effect, ushering in a new era of data protection in the EU. Organizations were required to comply with strict data protection standards, including provisions for data breach notification and fines for non-compliance. The GDPR's impact extends beyond the EU, influencing data protection practices globally. The study Eguia L. M. N. (Eguia, 2024) states that inconsistencies in assessing third countries' data protection systems could lead to challenges and questions regarding the validity of adequacy decisions, reminiscent of the period between Privacy Shield and EU-US DPF. Clear criteria, such as those outlined in Article 45(2) GDPR and A29WP Guidelines, are crucial for decision-makers and third countries seeking adequacy, fostering a more transparent and consistent process. The EC's efforts to re-approve pre-GDPR adequacy decisions and ongoing discussions with other countries underscore the need for continuous monitoring and alignment with GDPR standards to ensure the protection of EU data subjects' rights. Its emphasis on accountability, consent, and data portability has set a precedent for data protection laws worldwide. As organizations adapt to the GDPR's requirements, the regulation continues to shape

the digital landscape, ensuring the protection of individuals' privacy rights in an increasingly data-driven world.

5.2. Historical Foundation of the AI Act, 2024

The timeline of the Artificial Intelligence Act (AI Act) spanning from 2020 to 2024 illustrates a thorough process culminating in its final approval. In October 2020, the European Council initiated discussions on the digital transition, emphasizing the imperative of increased investments in AI research, innovation, and implementation, setting the groundwork for subsequent developments. In April 2021, the European Commission proposed the AI Act, with the aim of standardizing regulations concerning artificial intelligence and bolstering trust in AI technology. This proposal marked a significant stride towards establishing a regulatory framework for AI systems in the EU. Following this, on December 6, 2022, the Council endorsed its stance on the AI Act, underscoring its dedication to ensuring the safety of AI systems while upholding fundamental rights and EU values, thereby initiating negotiations with the European Parliament to achieve a consensus. The culmination of these deliberations took place on December 9, 2023, when the Council and the European Parliament reached a provisional agreement on the AI Act following rigorous negotiations. This landmark represented the world's first set of regulations for AI, stressing the importance of harmonizing rules to foster secure and ethically sound AI development. The agreement aimed at ensuring that AI systems in the EU market adhere to stringent safety standards and uphold fundamental rights. Overall, the history of the AI Act, 2024 demonstrates a concerted endeavor by EU institutions to tackle the challenges and opportunities presented by AI technology. From initial deliberations to the ultimate consensus, the process involved collaboration among diverse stakeholders to establish a regulatory framework that encourages innovation while safeguarding the rights and values of individuals. This comprehensive approach underscores the EU's dedication to fostering responsible AI development and deployment.

6. Comparative Studies

6.1. Key Differences between GDPR, 2016 and AI Act, 2024

Here is a detailed comparison between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024 across various key aspects:

A) Qualification of parties:

GDPR: Defines the roles of data controllers and data processors in handling personal data.

AI Act: Specifies the responsibilities of providers, users, and developers of artificial intelligence systems.

B) Human oversight and risk management system:

GDPR: Emphasizes human intervention in decision-making processes and requires risk assessments for data processing activities.

AI Act: Mandates human oversight in high-risk AI systems and requires risk assessments to evaluate impacts on rights and safety.

C) Impact assessments:

GDPR: Requires data protection impact assessments for risky data processing activities.

AI Act: Mandates risk assessments for high-risk AI systems to evaluate impacts on rights, safety, and security.

D) Special categories of personal data:

GDPR: Provides rules for processing sensitive personal data with additional safeguards.

AI Act: Addresses the handling of sensitive data within AI systems to prevent discrimination and ensure privacy protection.

E) Competent authorities:

GDPR: Establishes supervisory authorities in EU member states for data protection enforcement.

AI Act: Designates competent authorities at the EU level to oversee AI regulation and enforcement.

F) Key features:

GDPR: Focuses on data protection, transparency, accountability, and individual rights.

AI Act: Regulates the development, deployment, and use of AI systems, emphasizing ethical practices and human oversight.

G) Scope:

GDPR: Focuses on personal data protection and privacy rights.

AI Act: Specifically targets the regulation of artificial intelligence systems and their impact on various sectors.

H) Key definitions:

GDPR: Defines terms like personal data, data controller, and data processor.

AI Act: Introduces definitions for AI-related terms such as high-risk AI systems and human oversight.

I) Legal basis:

GDPR: Establishes principles for lawful processing of personal data.

AI Act: Sets legal requirements for AI system development and deployment.

J) Controller and processor obligations:

GDPR: Imposes obligations on data controllers and processors for data protection.

AI Act: Specifies obligations for AI providers, users, and developers to ensure ethical AI practices.

K) Individuals' rights:

GDPR: Grants rights such as data access, erasure, portability, and objection to processing.

AI Act: Ensures rights related to transparency, information, and human oversight in AI systems.

L) Enforcement:

GDPR: Empowers supervisory authorities to enforce data protection laws and impose fines.

AI Act: Establishes enforcement mechanisms, including penalties for non-compliance and oversight by competent authorities.

This comparison highlights the differences between the GDPR, 2016 and the AI Act, 2024 in terms of their focus, provisions, and implications for data protection and artificial intelligence regulation.

6.2. The AI Act, 2024 and the AILD, 2022

The European Parliament has placed a top priority on ensuring the safety, transparency, traceability, and non-discriminatory nature of all artificial intelligence (AI) systems used within the European Union (EU). This commitment aligns with the broader digital strategy of the EU, which emphasizes regulation and oversight of AI. Central to this effort is the definition of 'AI system,' crucial for shaping regulatory frameworks within the EU. The European Union's AI Liability Directive (AILD) aims to establish a fair compensation system for AI-related injuries, particularly in cases where the injury results from someone's fault rather than random errors. It introduces a "presumption of causality" to aid claimants, which can be rebutted by the defendant. Additionally, courts are empowered to demand disclosure of evidence related to high-risk AI systems. The AILD clarifies existing liability rules for AI, preventing undue burdens on businesses, especially those utilizing low-risk AI. Scheduled for review after five years, its effectiveness will be assessed. Overall, the AILD reflects the EU's commitment to regulating AI responsibly while ensuring fair compensation for any harm caused by AI systems.

7. Significance of AI Act, 2024, the AILD, 2022 and the GDPR, 2016

The AI Act of 2024 represents a landmark legislative milestone in the European Union's (EU) ongoing efforts to regulate artificial intelligence (AI) technologies. Enacted to ensure the ethical and responsible development and deployment of AI systems, the AI Act sets forth comprehensive rules governing AI across various sectors within the EU. It emphasizes the importance of transparency, accountability, and human oversight in AI systems, aiming to mitigate potential risks associated with AI while promoting innovation and competitiveness. Complementing the AI Act, the AI Liability Directive (AILD) of 2022 addresses the legal implications of AI-related harm by establishing a framework for non-contractual civil liability for AI systems. By introducing rules for fair compensation in cases where AI systems

cause harm due to human fault, the AILD aims to provide clarity and legal certainty for both AI developers and users. It also underscores the EU's commitment to safeguarding individuals' rights and interests in the rapidly evolving landscape of AI technology. Furthermore, the General Data Protection Regulation (GDPR) of 2016 lays a foundational framework for data protection and privacy rights within the EU. While not specifically focused on AI, the GDPR's principles of accountability, transparency, and data protection are highly relevant in the context of AI regulation. As AI systems often rely on vast amounts of personal data to function, the GDPR's provisions play a crucial role in ensuring that AI technologies comply with data protection standards and respect individuals' privacy rights. Together, the AI Act, AILD, and GDPR form a comprehensive regulatory framework that addresses various aspects of AI development, deployment, and accountability within the EU, reflecting the EU's commitment to fostering ethical and responsible AI innovation while safeguarding individuals' rights and interests.

8. Conclusion

The Artificial Intelligence Act of 2024 (AI Act) represents a significant legislative development in the European Union's approach to regulating artificial intelligence technologies and underscores the significance of social safety nets and re-skilling initiatives in mitigating job displacement while harnessing the potential of AI (Butt, 2024) to inform effective policymaking in advanced social welfare models and the role of artificial intelligence (AI) in driving productivity and economic growth becomes increasingly pertinent (Butt, 2024). The comprehensive regulation lays down harmonized rules for the deployment and use of AI systems across various sectors. The AI Act aims to ensure the ethical and responsible development of AI, emphasizing transparency, accountability, and human oversight in AI applications. It sets out requirements for high-risk AI systems, including data governance, risk assessment, and compliance mechanisms to safeguard fundamental rights and mitigate potential risks associated with AI technologies. On the other hand, the General Data Protection Regulation (GDPR) of 2016 is a landmark legislation that governs the protection and processing of personal data within the EU. The GDPR establishes rules for the lawful and fair treatment of individuals' personal information, emphasizing data privacy, security, and individual rights. It imposes obligations on organizations handling personal data, requiring them to implement appropriate technical and organizational measures to ensure data protection. The GDPR also grants individuals control over their personal data, including the right to

access, rectify, and erase their information, promoting transparency and accountability in data processing practices. Both the AI Act of 2024 and the GDPR of 2016 reflect the EU's commitment to fostering innovation while upholding fundamental rights and ethical standards in the digital age. These regulations work in tandem to create a regulatory framework that balances technological advancement with the protection of individuals' privacy and data rights, setting a global standard for AI governance and data protection practices.

9. Summary of Key Findings and Insights

The interaction between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024 within the context of data protection and privacy rights in AI technologies is multifaceted. The GDPR, aimed at protecting individuals' privacy rights and ensuring responsible data handling practices, intersects with the AI Act, which regulates the development and deployment of AI systems, particularly in high-risk scenarios. While both regulations share common goals of safeguarding fundamental rights and promoting ethical standards in technology, they also present challenges when implemented simultaneously, leading to potential clashes in certain aspects. The AI Act focuses on transparency, accountability, and human oversight to ensure the ethical use of AI technologies, setting out specific requirements for high-risk AI applications to mitigate potential harms and protect individuals' rights. On the other hand, the GDPR serves as a cornerstone for data protection and privacy rights, establishing rules for the lawful processing of personal data and imposing obligations on organizations to implement robust data protection measures. However, the simultaneous application of the AI Act and GDPR can lead to challenges and conflicts, especially concerning innovation and technological advancement versus stringent data protection requirements. The comparison of the GDPR and the AI Act across various key aspects highlights their complementary roles in shaping the digital landscape within the EU. While the GDPR prioritizes data protection, transparency, and individual rights, the AI Act addresses the challenges posed by AI systems, emphasizing ethical practices, human oversight, and risk management. However, differences in regulatory focuses and requirements can lead to clashes, particularly in areas where data protection principles intersect with AI development. Finding a harmonious balance between fostering AI innovation and protecting individuals' data privacy rights is crucial to navigating the potential clashes between these two regulatory frameworks. Organizations must carefully harmonize their practices to

meet the requirements of both regulations effectively, ensuring ethical and lawful AI development and deployment while upholding individuals' rights and values in the digital age. Ultimately, the coexistence of the AI Act and GDPR represents a significant step forward in addressing the challenges and opportunities presented by the digital revolution, positioning the EU as a global leader in data protection and AI regulation.

Q: How do the General Data Protection Regulation of 2016 (GDPR) and the Artificial Intelligence Act of 2024 (AI Act) interact in terms of data protection and privacy rights within the context of AI technologies, and to what extent do they complement each other in regulating the ethical and responsible development and deployment of AI systems within the European Union? Additionally, what potential areas of conflict or tension exist between these regulations, and how might they be addressed to ensure coherence and consistency in AI regulation, while considering their impact on businesses, organizations, and individuals operating within the EU?

R: The interaction between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024 within the context of data protection and privacy rights in AI technologies is multifaceted and critical in shaping the regulatory landscape of the European Union (EU). The GDPR, established in response to increasing concerns over data privacy and security, lays down comprehensive provisions for the processing, storage, and transfer of personal data. It emphasizes principles such as transparency, accountability, and individual rights, aiming to protect individuals' privacy rights and ensure responsible data handling practices by organizations. On the other hand, the AI Act, enacted to regulate the development and deployment of AI technologies, intersects with the GDPR in several key areas related to data protection and privacy rights. Firstly, the AI Act incorporates provisions that require AI systems to comply with the principles outlined in the GDPR, ensuring that data processing activities conducted by AI systems adhere to data protection standards and respect individuals' privacy rights. This alignment between the GDPR and the AI Act serves to reinforce the importance of data protection and privacy considerations in AI development and deployment processes. Secondly, the AI Act introduces specific requirements for transparency and accountability in AI systems, which are closely linked to data protection and privacy rights. For example, the AI Act mandates that high-risk AI systems must be accompanied by documentation detailing their capabilities, limitations, and potential impact on individuals' rights, including privacy rights. By enhancing transparency

and accountability in AI systems, the AI Act aims to ensure that individuals are informed about how their data is being processed and used, thereby contributing to the protection of their privacy rights as stipulated in the GDPR. Furthermore, the AI Act also emphasizes the importance of human oversight in AI systems, particularly those deemed high-risk. This requirement aligns with the GDPR's emphasis on human intervention in decision-making processes involving personal data, ensuring that individuals retain control over decisions that may affect their privacy rights. Additionally, the AI Act mandates risk assessments for high-risk AI systems, which include an evaluation of potential risks to individuals' rights, including privacy rights. By integrating risk assessment processes into AI development and deployment, the AI Act seeks to identify and mitigate potential privacy risks, thereby enhancing the protection of individuals' privacy rights in the context of AI technologies. Overall, the interaction between the GDPR and the AI Act in terms of data protection and privacy rights within the context of AI technologies is characterized by alignment, reinforcement, and enhancement of existing data protection standards and principles. By incorporating data protection and privacy considerations into AI regulation, the GDPR and the AI Act collectively contribute to the establishment of a robust regulatory framework that safeguards individuals' privacy rights while promoting responsible and ethical AI development and deployment within the EU. Regarding potential areas of conflict or tension between these regulations, the differing regulatory focuses and requirements of the GDPR and the AI Act can lead to clashes, particularly in areas where data protection principles intersect with AI development. The GDPR's emphasis on principles such as data minimization, purpose limitation, and individual rights may conflict with the AI Act's objectives of fostering innovation and technological advancement in AI systems. For example, AI systems often require access to large datasets for training purposes, raising concerns about compliance with GDPR requirements regarding data processing and consent. Additionally, the GDPR's emphasis on individual rights, such as the right to data access and erasure, may conflict with the AI Act's provisions for data retention and processing necessary for AI model training and improvement. Furthermore, the AI Act's requirements for human oversight and transparency in AI decision-making processes may clash with the GDPR's principles of automated decision-making transparency and the right to explanation. To address these conflicts, a nuanced approach is necessary to balance the objectives of both regulations while ensuring coherence and consistency in AI regulation. This could involve establishing clear guidelines and standards for AI developers to ensure compliance with both the GDPR and the AI Act, including technical solutions for

data anonymization and privacy-preserving AI techniques. Additionally, enhancing collaboration and coordination between regulatory authorities responsible for enforcing the GDPR and the AI Act can help ensure consistency in regulatory interpretation and enforcement. This may involve establishing cross-functional working groups or regulatory bodies tasked with addressing AI-specific data protection challenges and promoting best practices for AI governance. Moreover, providing businesses, organizations, and individuals with clear guidance and support for navigating the regulatory landscape can help mitigate potential conflicts and ensure compliance with both regulations, such as offering educational resources, training programs, and compliance assistance tailored to the unique challenges and requirements of AI development and deployment. Ultimately, ensuring coherence and consistency in AI regulation requires a collaborative and adaptive approach that takes into account the evolving nature of AI technologies and the complex interplay between data protection principles and AI development. By addressing potential areas of conflict proactively and promoting harmonization between the GDPR and the AI Act, policymakers can foster innovation and responsible AI adoption while safeguarding the rights and interests of individuals operating within the EU.

10. Future Directions for Research

As the regulatory landscape surrounding data protection and artificial intelligence (AI) continues to evolve, there are several key areas that warrant further exploration to deepen our understanding of the interaction between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024.

- **Long-term Impact Assessment:** Future research could focus on conducting longitudinal studies to assess the long-term impact of the GDPR and the AI Act on businesses, organizations, and individuals operating within the European Union (EU). This could involve examining trends in data protection compliance, AI adoption rates, innovation outcomes, and the overall economic and social implications of these regulations over time.

- **Ethical and Societal Implications:** There is a need for research that delves into the ethical and societal implications of AI technologies regulated under the AI Act within the framework of the GDPR. This includes exploring issues such as algorithmic bias, discrimination, fairness, accountability, and the broader societal implications of AI-driven decision-making processes on individuals and communities.

- **Governance and Enforcement Mechanisms:** Further research could investigate the effectiveness of governance and enforcement mechanisms established under the GDPR and the AI Act. This includes examining the role of regulatory authorities, enforcement actions taken against non-compliant entities, and the challenges associated with cross-border enforcement and cooperation in the context of AI technologies.

- **Technological Innovation and Adaptation:** As AI technologies continue to advance rapidly, future research could explore how the GDPR and the AI Act adapt to technological innovations and emerging AI applications. This includes examining the regulatory challenges posed by novel AI use cases, such as autonomous vehicles, healthcare diagnostics, and predictive policing, and identifying strategies to address these challenges while upholding data protection and privacy rights.

- **International Comparisons and Harmonization Efforts:** Comparative studies across different jurisdictions could provide valuable insights into the similarities and differences in regulatory approaches to data protection and AI governance. Additionally, research on international harmonization efforts aimed at aligning data protection and AI regulations globally could help inform future policy development and promote interoperability between regulatory frameworks.

- **Stakeholder Perspectives and Public Perception:** Future research could explore stakeholder perspectives and public perception of the GDPR and the AI Act, including the views of businesses, policymakers, civil society organizations, and the general public. Understanding stakeholder attitudes and perceptions can inform regulatory decision-making processes and help identify areas for improvement or refinement in existing regulations.

By addressing these future research directions, scholars can contribute to a deeper understanding of the dynamic interplay between data protection and AI regulation, paving the way for more effective and adaptive regulatory frameworks that promote responsible AI development and safeguard individuals' rights and interests in an increasingly data-driven and AI-powered world.

11. Challenges and Considerations

Navigating the intersection between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024 presents several challenges and considerations for policymakers, businesses, organizations, and individuals within the European Union (EU).

- **Regulatory Divergence:** The GDPR and the AI Act have distinct regulatory objectives and requirements, potentially leading to inconsistencies and conflicts in their implementation. Balancing the principles of data protection and privacy rights with the promotion of innovation and responsible AI development poses a significant challenge for ensuring coherence and consistency in AI regulation.

- **Data Privacy and AI Development:** The GDPR's emphasis on data protection and privacy rights may impose constraints on AI development processes, particularly regarding data collection, processing, and consent requirements. Finding a balance between protecting individuals' privacy rights and facilitating AI innovation is crucial but challenging.

- **Transparency and Accountability:** Both the GDPR and the AI Act emphasize transparency and accountability in data processing and AI decision-making processes. However, reconciling the GDPR's requirements for human oversight and explanation with the AI Act's objectives of promoting AI autonomy and efficiency poses a challenge in ensuring transparency and accountability in AI systems.

- **Ethical and Responsible AI Deployment:** Ensuring that AI systems deployed within the EU adhere to ethical principles and respect fundamental rights is essential. However, translating ethical considerations into actionable regulatory measures while avoiding stifling innovation presents a complex challenge for policymakers and regulators.

- **Compliance Burden:** Businesses and organizations operating within the EU face a significant compliance burden in adhering to both the GDPR and the AI Act's requirements. Developing and implementing processes and technologies that comply with both sets of regulations while maintaining operational efficiency and competitiveness is a considerable challenge.

- **International Cooperation:** Given the global nature of AI technologies and data flows, achieving harmonization and interoperability between the GDPR and international AI regulations presents challenges for international cooperation and coordination efforts.

Addressing these challenges and considerations requires a collaborative and adaptive approach from policymakers, regulators, businesses, organizations, and individuals. Striking a balance between data protection, privacy rights, and AI innovation, while fostering transparency, accountability, and ethical AI deployment, is essential for realizing the potential benefits of the GDPR and the AI Act as a power couple rather than a clash of titans.

12. Recommendations for Policy and Practice

In light of the intricate relationship between the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024, several recommendations for policy and practice emerge to ensure coherence and consistency in AI regulation while safeguarding data protection and privacy rights within the European Union (EU).

- **Harmonization of Regulations:** Policymakers should prioritize the harmonization of the GDPR and the AI Act to streamline regulatory requirements and mitigate potential conflicts. This entails conducting comprehensive assessments of existing regulations to identify areas of misalignment and developing clear guidelines and standards for AI developers to ensure compliance with both sets of regulations.

- **Enhanced Collaboration:** Policymakers should enhance collaboration and coordination between regulatory authorities responsible for enforcing the GDPR and the AI Act. Establishing cross-functional working groups or regulatory bodies can facilitate communication and knowledge-sharing, enabling a more coherent approach to AI regulation and enforcement.

- **Investment in Privacy-Preserving Technologies:** Policymakers should invest in research and development initiatives to promote the development of privacy-preserving AI technologies and tools. By incentivizing the adoption of privacy-enhancing techniques and methodologies, policymakers can address concerns regarding data protection and privacy rights while promoting innovation in AI development and deployment.

- **Educational Resources and Training**: Policymakers should prioritize the development of educational resources and training programs to support businesses, organizations, and individuals in navigating the regulatory landscape. Providing clear guidance on compliance requirements and best practices for AI governance can

help mitigate potential conflicts and ensure responsible AI development and deployment.

- **Regular Reviews and Assessments:** Policymakers should conduct regular reviews and assessments of the GDPR and the AI Act to adapt regulations to the evolving landscape of AI technologies and data protection challenges. This iterative approach to regulation can ensure that regulatory frameworks remain relevant, effective, and aligned with societal values and human rights principles.

By implementing these recommendations, policymakers can foster a more coherent and consistent regulatory framework for AI within the EU, promoting responsible and ethical AI development while safeguarding data protection and privacy rights for individuals.

13. Limitation

In delving into the intersection of the General Data Protection Regulation (GDPR) of 2016 and the Artificial Intelligence Act (AI Act) of 2024, it is essential to acknowledge the limitations of existing studies in this field. Firstly, while there is a growing body of literature exploring the individual implications of the GDPR and the AI Act, there is a notable scarcity of research comprehensively examining their interaction and potential conflicts. This gap in the literature highlights the need for further empirical studies and interdisciplinary research that consider the complex interplay between data protection regulations and AI governance. Additionally, much of the existing literature tends to focus on legal and regulatory perspectives, overlooking broader societal implications and stakeholder perspectives. Consequently, there is a need for studies that adopt a more holistic approach, considering the perspectives of policymakers, businesses, civil society, and individuals affected by these regulations. Moreover, given the relatively recent enactment of the AI Act in 2024, there is limited empirical evidence available on its practical implementation and impact on businesses, organizations, and individuals operating within the EU. Future research should aim to address this gap by conducting longitudinal studies and empirical assessments to evaluate the effectiveness and challenges of the AI Act in regulating AI technologies. Furthermore, the dynamic nature of both the GDPR and the AI Act necessitates ongoing research to keep pace with technological advancements, regulatory updates, and evolving societal attitudes towards data protection and AI governance. In conclusion, while existing studies provide valuable insights into the individual

regulatory frameworks of the GDPR and the AI Act, there is a need for further research that explores their interaction, societal implications, and practical implementation to inform effective policymaking and regulatory compliance strategies.

14. Ethical Consideration

Navigating the intricate relationship between data protection and artificial intelligence (AI) regulation necessitates a commitment to ethical principles that uphold individual rights, fairness, and transparency in AI technologies. The GDPR sets a firm ethical groundwork for data processing within the European Union (EU), emphasizing accountability, transparency, and the protection of fundamental rights. It prioritizes principles like informed consent, data minimization, and purpose limitation, reflecting a dedication to ethical data management practices that respect individuals' privacy and autonomy. Similarly, the AI Act of 2024 builds upon these ethical foundations, extending them to the domain of AI development and deployment. By highlighting the significance of human oversight, transparency, and risk management in AI systems, the AI Act aims to ensure that AI technologies operate in accordance with societal values and human rights. It introduces mandates for documentation, accountability, and risk assessment, with the goal of enhancing transparency and mitigating potential risks to individuals' rights, including privacy rights. The convergence of the GDPR and the AI Act regarding ethical considerations underscores a shared commitment to responsible and ethical AI advancement and implementation within the EU. Through the alignment of regulatory goals and the promotion of ethical data handling practices, these regulations jointly contribute to establishing a robust ethical framework that safeguards individual rights while fostering innovation and technological progress. Nevertheless, as we navigate the complexities of AI regulation and data protection, it remains crucial to maintain vigilance and proactively address emerging ethical challenges. This ensures that AI technologies continue to serve the common good while adhering to ethical standards and principles.

About Author

The author Junaid Sattar Butt possesses a distinguished academic background, including a Master of Laws (LL.M) with honors from the University of Lahore, specializing in International & Comparative Laws and Research Methodology. He also holds a Master of Arts in Political Science from the University of the Punjab, Lahore, and a Bachelor of Laws (LL.B) from the same institution, providing him with a comprehensive understanding of legal principles. Author's educational journey extends to a Master of Business Administration (Finance) from the Virtual University of Pakistan, enhancing his expertise in financial matters. Proficient in English, Urdu and Punjabi, Butt has developed essential communication and organizational skills throughout his academic and professional endeavors. In terms of professional experience, Mr. Butt has over four years of practical experience as an Advocate at the High Court and District Courts, where he has honed his skills in legal research, court assistance, settlements, and arbitration. The author has also served as a Visiting Teaching Faculty member, imparting knowledge on International Laws, Administrative Laws, and Human Rights. Additionally, his role as a Law/Research Officer at Malik Law Associates has further solidified his proficiency in legal research and case preparation. Butt's research profile demonstrates his dedication to exploring contemporary legal issues. His publications cover diverse topics such as the impact of digitalization on administrative decision-making processes, comparative studies on international relations, human rights protection, and political instability. The author actively participates in conferences, seminars, and workshops, showcasing his commitment to continuous learning and professional development. Butt's involvement in legal advocacy and community engagement initiatives, as evidenced by his memberships in various bar associations and committees, reflects his dedication to advancing justice and social welfare. With his strong academic background, extensive professional experience, and commitment to legal scholarship and advocacy, the author is well-equipped to pursue doctoral research in the field of law and governance, contributing significantly to the advancement of legal knowledge and practice.

Acknowledgment

The author expresses his sincere gratitude to the learned editorial board for their invaluable support during the research publication process. The author also express their deepest gratitude to their late father, Mr. Abdul Sattar Butt, for his unwavering

guidance and encouragement throughout the journey. His wisdom, patience, and dedication have been a constant source of inspiration, shaping the author into the person he is today. The author is profoundly grateful her mother Mst. Nighat Firdous for her endless support and her sacrifices and lessons, and for her love and devotion, which have been a beacon of strength. Her presence in the author's life is a blessing beyond measure.

Declaration of Conflicting Interests

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

References

Antonaros, V. (24 April, 2024). *The Intersection of AI Law with the GDPR: Ensuring Data Protection in Artificial Intelligence Systems*. Retrieved from https://repository.ihu.edu.gr//xmlui/handle/11544/30371.

Asatiani, A.; Copeland, O. & Penttinen, E. (2023). Deciding on the robotic process automation operating model: A checklist for RPA managers. *Business Horizons*, Vol. 66(1), pp. 109-121.

Bauroth, M.; Rath-Manakidis, P.; Langholf, V.; Wiskott, L. & Glasmachers, T. (2024). tachAId—An interactive tool supporting the design of human-centered AI solutions. *Frontiers in Artificial Intelligence, 7*. Retrieved from https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2024.1354114/full.

Borgesius, F. Z.; Hacker, P.; Baranowska, N. & Fabris, A. (2024). Non-discrimination law in Europe: a primer for non-lawyers. *Elsevier Analytical Services Research Paper Series*. Retrieved from https://ssrn.com/abstract=4786956.

Bratu, I. & Leiser, M. (2024). Navigating the convergence of law, computers & technology. *International Review of Law, Computers & Technology*, pp. 1-3.

Butt, J. (2023). A Comparative Analysis of the Regulatory Approach And Management Practice For Digital Currencies, And the Role Of International Financial Organizations, In Developing A Global Regulatory Framework For Accounting Standards of Digital Crypto-Currency. *The Journal of Accounting and Management*, Vol. 13(3), pp. 7-21. Retrieved from https://dj.univ-danubius.ro/index.php/JAM/article/view/2586.

Matheson, L. L. P. (15 January, 2024). *CJEU provides clarity on right to compensation for GDPR infringements. European Union*. Retrieved from https://www.lexology.com/library/detail.aspx?g=f4989994-f25d-4363-875a-beee197d2378.

Butt, J. (2023). The Impact of Artificial Intelligence (AI) on the Efficiency of Administrative Decision Making Including Ethical & Legal Considerations and Comparative Study about Countries Already

Incorporated AI for Administrative Decisions. *The Acta Universitatis Danubius. Juridica,* Vol. 19(3), pp. 7-25. Retrieved from https://dj.univ-danubius.ro/index.php/AUDJ/article/view/2560.

Butt, J. (2024). Analytical Study of the World's First EU Artificial Intelligence (AI) Act. *International Journal of Research Publication and Reviews,* Vol. 5(3), pp. 7343-7364.

Butt, J. (2024). The Impact of Digitalization (AI) On Administrative Decision-Making Processes and Access to Justice– A Nordic Perspective. *Acta Universitatis Danubius. Juridica,* Vol. 20(1), pp. 22–42. Retrieved from https://dj.univ-danubius.ro/index.php/AUDJ/article/view/2712.

Butt, J. (2024). The Role of Artificial Intelligence (AI) In Productivity & Economic Growth in Nordic Welfare States. *Acta Universitatis Danubius. Œconomica,* Vol. 20(2). Retrieved from https://dj.univ-danubius.ro/index.php/AUDOE/article/view/2714.

Byanjankar, A.; Mezei, J. & Heikkilä, M. (2021). Data-driven optimization of peer-to-peer lending portfolios based on the expected value framework. *Intelligent Systems in Accounting, Finance and Management,* Vol. 28(2), pp. 119-129. Retrieved from https://onlinelibrary.wiley.com/doi/10.1002/isaf.1490.

Cabrera, L. (13 March, 2024). *EU's much-heralded AI Act agreed by EU Parliament – but serious human rights holes in law remain*. Retrieved from Euractiv: https://www.euractiv.com/section/artificial-intelligence/opinion/eus-much-heralded-ai-act-agreed-by-eu-parliament-but-serious-human-rights-holes-in-law-remain/.

Christof, W.; Jonas, F.; Hinz, O. & Wil, M. P. (2024). Digital Democracy: A Wake-Up Call. *Business & Information Systems Engineering,* Vol. 66, pp. 127–134.

Collan, M.; Savolainen, J.; Virolainen, V. & Luukka, P. (2023). A Vision for a Highly Automated Digital Local Manufacturing Network—Solutions and Challenges. In Huang, C.; Dekkers, R.; Chiu, S. Popescu, D. & Quezada, L. *Intelligent and Transformative Production in Pandemic Times*, pp. 377–384. Retrieved from https://link.springer.com/chapter/10.1007/978-3-031-18641-7_36.

Cowley, B.; Charles, D.; Pfuhl, G. & Rusanen, A. (2023). Artificial Intelligence in Education as a Rawlsian Massively Multiplayer Game: A Thought Experiment on AI Ethics. In Niemi, H.; Pea, R. & Lu, Y. *AI in Learning: Designing the Future. Springer, Cham.*

Davoodi, L. & Mezei, J. (2022). Comparative Study of Machine Learning Models for Sentiment Analysis: Customer Reviews of E-commerce Platforms. In Pucihar, A.; Kljajić, M. B.; Bons, R.; Sheombar, A.; Ongena, G. & Vidmar, D. *35th Bled eConference: Digital Restructuring and Human (Re)Action.*

Díaz-Rodríguez, N.; Del Ser, J.; Coeckelbergh, M.; López de Prado, M.; Herrera-Viedma, E. & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion,* Vol. 99, pp. 1-24.

Duflot, A. (2024). Artificial Intelligence in the French Law of 2024. *Legal Issues in the Digital Age,* Vol. 5(1), pp. 37-56.

Earley, S.; Henderson, D. & Association, D. M. (2017). *DAMA-DMBOK: Data Management Body of Knowledge.* New Jersey: Technics Publications. Retrieved from https://pdfcoffee.com/dama-

international-dama-dmbok-2nd-edition-data-management-body-of-knowledge-technics-publications-2017pdf-4-pdf-free.html.

Eguia, L. M. (2024). *The Magical Mystery Data Transfer Mechanism: An insight into how the adequacy of a third country is determined under Article 45(2) GDPR (Master's thesis).* Retrieved from https://www.duo.uio.no/bitstream/handle/10852/110615/8/ICTLTHESIS_9014_H23.pdf.

Erkkilä, T. (2024)). Hybridity in digital and algorithmic public governance. In Giuseppe, G. & Jarmo, V. *Handbook of Accounting and Public Governance*, pp. 32-46. Edward Elgar Publishing. Retrieved from https://www.ippapublicpolicy.org/file/paper/60da17e9ae141.pdf.

*** (2024). *European Data Protection Supervisor*. Retrieved from The History of the General Data Protection Regulation: https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

Fresz, B.; Dubovitskaya, E.; Brajovic, D.; Huber, M. & Horz, C. (2024). How should AI decisions be explained? *Requirements for Explanations from the Perspective of European Law*, pp. 1-18. Retrieved from https://arxiv.org/pdf/2404.12762.

Gkritsi, E. (2024). *AI Act's global effects might be overstated, experts say*. Retrieved from Euractiv: https://www.euractiv.com/section/artificial-intelligence/news/ai-acts-global-effects-might-be-overstated-experts-say/.

Green, D. (2024). Strategic Indeterminacy and Online Privacy Policies: (Un)informed Consent and the General Data Protection Regulation. *International Journal of Semiotics of Law*, pp. 1-29.

Gritsenko, D. & Wood, M. (2022). Algorithmic governance: A modes of governance approach. *Regulation & Governance*, Vol. 16(1), pp. 45-62. Retrieved from https://www.researchgate.net/publication/346876996_Algorithmic_governance_A_modes_of_governance_approach.

G'sell, F. (2024). An Overview of the European Union Framework Governing Generative AI Models and Systems. *Elsevier Analytical Services Research Paper Series*, pp. 1-102. Retrieved from https://ssrn.com/abstract=4762804 or http://dx.doi.org/10.2139/ssrn.4762804.

Hakobyan, M. (2024). *Artificial Intelligence rulebook fails to stop proliferation of abusive technologies.* Retrieved from Amnesty international. https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/.

Hallamaa, J. & Kalliokoski, T. (2022). AI Ethics as Applied Ethics. *Frontiers in computer science*, Vol. 4. Retrieved from https://www.researchgate.net/publication/359803298_AI_Ethics_as_Applied_Ethics.

Harju, A.; Hallikas, J.; Immonen, M. & Lintukangas, K. (2023). The impact of procurement digitalization on supply chain resilience: empirical evidence from Finland. *Supply Chain Management*, Vol. 28(7), pp. 62-76. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/SCM-08-2022-0312/full/html.

Kalliokoski, T. (2023). Intelligence Biological understanding is needed in the development of technologies. *Theological Journal*, Vol. 128(2), pp. 121-122. Retrieved from https://helda.helsinki.fi/server/api/core/bitstreams/37085aa7-76de-4095-8fff-4a4e7cbf43d9/content.

Kalsi, M. (2024). Still losing the race with technology? Understanding the scope of data controllers' responsibility to implement data protection by design and by default. *International Review of Law, Computers & Technology*, pp. 1–23.

Karttunen, E.; Lintukangas, K. & Hallikas, J. (n.d.). Digital transformation of the purchasing and supply management process. *International Journal of Physical Distribution & Logistics Management*, Vol. 53(5/6), pp. 685-706. Retrieved from https://www.emerald.com/insight/content/doi/10.1108/IJPDLM-06-2022-0199/full/html.

Khakurel, J. & Blomqvist, K. (2022). Artificial Intelligence Augmenting Human Teams. A Systematic Literature Review on the Opportunities and Concerns. In Degen, H. & Ntoa, S. *Artificial Intelligence in HCI. HCII 2022. Lecture Notes in Computer Science* Vol. 13336. Retrieved from https://www.researchgate.net/publication/360600948_Artificial_Intelligence_Augmenting_Human_Teams_A_Systematic_Literature_Review_on_the_Opportunities_and_Concerns.

Khalfa, R.; Theinert, N. & Hardyns, W. (2024). From human intervention to meaningful human oversight? Mapping the opportunities and constraints in the decision-making process of place-based big data policing. *AI-Experiences and public safety.* Rotterdam, The Netherlands.

Koivisto, I. (2023). *Automated decision making is coming - are you ready?* Retrieved from Constitution blog: https://perustuslakiblogi.wordpress.com/2023/03/02/ida-koivisto-automaattinen-paatoksenteko-tulee-oletko-valmis/

Korpisaari (ex. Tiilikka), P. (2022). In Teoksessa, A.-S. & Pihlajarinne, T. *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities*, pp. 61-91. Retrieved from https://www.elgaronline.com/edcollchap/edcoll/9781839109966/9781839109966.00009.xml.

Kosurko, A.; Arminen, I.; Herron, R.; S. M. & Stevanovic, M. (2021). Observing Social Connectedness in a Digital Dance Program for Older Adults: An EMCA Approach. In Gao, Q. Z. *Human Aspects of IT for the Aged Population. Technology Design and Acceptance. HCII 2021. Lecture Notes in Computer Science*, Vol. 12786. Retrieved from https://helda.helsinki.fi/server/api/core/bitstreams/58fa92ee-3f55-4a26-a5a4-ac1bbc6b8dc6/content.

Kruse, N.; Wachter, P. & Schöning, J. (2024). Compliance of agricultural AI systems – app-based legal verification throughout the development. *P344 - 44th GIL Annual Conference 2023 - Focus: Promoting biodiversity through digital agriculture*, pp. 119-130. Retrieved from https://dl.gi.de/items/03873650-c7ea-4aaf-b91e-324ca7bafc1f.

Lamberg, J.-A. & Luoma, J. (2021). Ideology in Vicarious Learning–Related Communication. *Organization Science*, Vol. 32(3), pp. 708-730.

Laukkanen, T.; Laukkanen, T.; Xi, N.; Xi, N.; Hallikainen, H.; Hallikainen, H. & Hamari, J. (2021). Virtual technologies in supporting sustainable consumption: From a single-sensory stimulus to a multi-sensory experience. *International Journal of Information Management*, Vol. 63(4). Retrieved from https://www.researchgate.net/publication/356121754_Virtual_technologies_in_supporting_sustainable_consumption_From_a_single-sensory_stimulus_to_a_multi-sensory_experience#fullTextFileContent.

Leikin, E.; Riede, L.; Hofer, M. & Sue,N. G, (2024.). *Technology Disputes and Arbitration.* Retrieved from The European Arbitration Review. https://globalarbitrationreview.com/review/the-european-arbitration-review/2024/article/technology-disputes-and-arbitration.

Lynch, S. (2024). *Davos 2024: Six Takeaways on the AI Conversation at WEF*. Retrieved from The World Economic Forum: https://hai.stanford.edu/news/davos-2024-six-takeaways-ai-conversation-wef.

Mäkelä, E.; Lagus, K.; Lahti, L.; Säily, T.; Tolonen, M.; Hämäläinen, M.; Nevalainen, T. (2020). Wrangling with non-standard data. In Reinsone, S.; Skadiņa, I.; Baklāne, A. & Daugavietis, J. *Proceedings of the Digital Humanities in the Nordic Countries 5th Conference*, pp. 91-96. Retrieved from http://ceur-ws.org/Vol-2612/paper6.pdf.

Mesinovic, M. (2024). Explainability and the Law: Needs and Requirements. *Elsevier Analytical Services Research Paper Series*. Retrieved from https://ssrn.com/abstract=4808607.

Miller, K. (2024). *Spotting Visual Signs of Gentrification at Scale. Economy and Markets*. Retrieved from https://hai.stanford.edu/news/spotting-visual-signs-gentrification-scale.

Mlynář, J. & Arminen, I. (2023). Respecifying social change: the obsolescence of practices and the transience of technology. *Frontiers in Sociology*, Vol. 8. Retrieved from https://www.frontiersin.org/articles/10.3389/fsoc.2023.1222734/full#h8.

Nadeem, M.; Ali, Y.; Rehman, O. U. & Saarinen, L. T. (2023). Barriers and Strategies for Digitalisation of Economy in Developing Countries: Pakistan, a Case in Point. *Journal of the Knowledge Economy*, Vol. 15.

Nguyen, Q.; Tran, D. T.; Kanniainen, J.; Iosifidis, A. & Gabbouj, M. (2023). Cryptocurrency Portfolio Optimization by Neural Networks. *IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 25-32. Retrieved from https://ieeexplore.ieee.org/document/10371855/authors#authors.

Nikunen, K. (2023). The threat and allure of data capitalis. *Media & Communication*, Vol. 46(2), pp. 115–117.

Oinas, S. & Hotulainen, R. (2022). Remote learning experiences when you prefer pen & paper over digital devices. *Proceedings of Society for Information Technology & Teacher Education International Conference*, pp. 776-781. San Diego, United States: Association for the Advancement of Computing in Education (AACE). Retrieved Martie 25, 2024, from https://www.learntechlib.org/primary/p/220811/.

Parkatti, A.; Saari, T.; Tammelin, M. & Villi, M. (2022). Framing digital competence in media work – The case of Finland. *International Journal of Sociology and Social Policy*, Vol. 42(13/14), pp. 15-29.

Pathak, M. (2024, February 6). Data Governance Redefined: The Evolution of EU Data Regulations from the GDPR to the DMA, DSA, DGA, Data Act and AI Act. *Elsevier Analytical Services Research Paper Series*. Retrieved from https://ssrn.com/abstract=4718891 or http://dx.doi.org/10.2139/ssrn.4718891.

Peeters, B. (2024). Editorial: European Law Restrictions on Tax Authorities' Use of Artificial Intelligence Systems: Reflections on Some Recent Developments. *EC Tax Review*, Vol. 33(2), pp. 54-57. Retrieved from https://kluwerlawonline.com/journalarticle/EC+Tax+Review/33.2/ECTA2024006.

Picht, P. & Richter, H. (2022). EU Digital Regulation 2022: Data Desiderata. *GRUR International*, Vol. 71(5), pp. 395–402. Retrieved from https://doi.org/10.1093/grurint/ikac021.

Pihlajarinne, T. & Alen-Savikko, A. (2022). Conclusions on artificial intelligence, media and regulation. In Pihlajarinne, T. & Alén-Savikko A. *Artificial Intelligence and the Media: Reconsidering Rights and Responsibilities*, pp. 296-299. Edward Elgar.

Polyzou, F. (2024). *The draft AI Act through the lens of the GDPR (Master's thesis).* University Center of International Programmes of Studies, School of Humanities, Social Sciences and Economics. Retrieved from https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/30378/Fani%20Polyzou%20%281%29.pdf?sequence=1.

Premathilake, G.; Li, H.; Liu, Y. & Helander, N. (2021). *A Review of the Empirical Literature on Service Robots in Information Systems Literature*. Retrieved from http://urn.fi/URN:NBN:fi:tuni-202108186636.

Rantanen, V. & Komp-Leukkunen, K. (2023). Self-employment and Adaptation to Transformative Digitalization during Later Working Life. *Nordic Journal of Working Life Studies*, Vol. 14(S12).

Romero-Moreno, F. (2024). Generative AI and deepfakes: a human rights approach to tackling harmful content. *International Review of Law, Computers & Technology*, pp. 1–30. Retrieved from https://doi.org/10.1080/13600869.2024.2324540.

Ruohonen, J. & Mickelsson, S. (2023). Reflections on the Data Governance Act. *Digital Society*, Vol. 2.

Sankari, S.; Koulu, R.; Hirvonen, H. & Heikkinen, T. (2023). Artificial intelligence and the law: can we and should we regulate AI systems. In Brożek, B.; Kanevskaia, O. & Pałka, P. *Research Handbook on Law and Technology*, pp. 427-449. Edward Elgar. Retrieved from https://www.elgaronline.com/edcollchap/book/9781803921327/chapter26.xml.

Schutte, S.; Majewski, L. & Havu, K. (2021). Damages Liability for Harm Caused by Artificial Intelligence – EU Law in Flux. *Helsinki Legal Studies Research Paper*, Vol. 69. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897839.

Sharon, T. & Gellert, R. (2023). Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy. *Information, Communication & Society*, pp. 1–18.

Siitonen, M.; Laajalahti, A. & Venäläinen, P. (2024). Mapping Automation in Journalism Studies 2010–2019: A Literature Review. *Journalism Studies*, Vol. 3, pp. 299-318. Retrieved from https://converis.jyu.fi/converis/portal/detail/Publication/197574764?lang=en_GB.

Sjödin, D.; Liljeborg, A. & Mutter, S. (2024, March). Conceptualizing ecosystem management capabilities: Managing the ecosystem-organization interface. *Technological Forecasting and Social Change*, Vol. 200(1), pp. 123-187. Retrieved from https://www.researchgate.net/publication/378641715_Conceptualizing_ecosystem_management_capabilities_Managing_the_ecosystem-organization_interface.

Stark, A.; Ferm, K.; Hanson, R.; Johansson, M.; Khajavi, S.; Medbo, L. & Holmström, J. (2023). Hybrid digital manufacturing: Capturing the value of digitalization. *Journal of Operations Management*, Vol. 69(6), pp. 890-910. Retrieved from https://onlinelibrary.wiley.com/doi/10.1002/joom.1231.

Stockman, C.; O'Connell, A. & Nottingham, E. (2024). When it's cute but also dark: critical analysis of FarmVille 3's game design in the digital economy. *International Review of Law, Computers & Technology*, pp. 1–23.

Susarla, A. (2024). *The conversation*. Retrieved from Generative AI could leave users holding the bag for copyright violations: https://theconversation.com/generative-ai-could-leave-users-holding-the-bag-for-copyright-violations-225760.

Toset, S.; Late, E. & Kumpulainen, S. (2023, December 15). More than data repositories: perceived information needs for the development of social sciences and humanities research infrastructures. *Information Research an International Electronic Journal*, Vol. 28(4), pp. 83–101. Retrieved from https://informationr.net/infres/article/view/598.

van Gerven, M. (2022). Studying social policy in the digital age. In Nelson,K.; Nieuwenhuis, R. & Yerkes, M. *Social Policy in Changing European Societies*, pp. 251-264. Retrieved from https://www.elgaronline.com/edcollchap-oa/book/9781802201710/book-part-9781802201710-25.xml.

van Zoonen, W. S. & Treem, J. W. (2024). Algorithmic management of crowdworkers: Implications for workers' identity, belonging, and meaningfulness of work. *Computers in Human Behavior*, Vol. 152.

Vellinga, N. E. (2024). Rethinking compensation in light of the development of AI. *International Review of Law, Computers & Technology*, pp. 1–22.

Viljanen, M. & Parviainen, H. (2022). AI Applications and Regulation: Mapping the Regulatory Strata. *Frontiers in Computer Science*, Vol. 3. Retrieved from https://www.frontiersin.org/articles/10.3389/fcomp.2021.779957/full.

Weismann, M. F. (2024). Getting global cooperation right on internet governance: strategic roadmaps for the future. *International Review of Law, Computers & Technology*, pp. 1–27.

Wingström, R.; Hautala, J. & Lundman, R. (2022). Redefining Creativity in the Era of AI? Perspectives of Computer Scientists and New Media Artists. *Creativity Research Journal*, Vol. 36(2), pp. 177-193. Retrieved from https://www.tandfonline.com/doi/epdf/10.1080/10400419.2022.2107850?needAccess=true.

Wolff, J.; Lehr, W. & Yoo, C. S. (2023, August 1). Lessons from GDPR for AI Policymaking. *Virginia Journal of Law & Technology*, Vol. 27. Retrieved from SSRN: https://ssrn.com/abstract=4528698.

Yigit, Y.; Buchanan, W. J.; Tehrani, M. G. & Maglaras, L. (2024). *Review of Generative AI Methods in Cybersecurity*. Retrieved from https://arxiv.org/html/2403.08701v2#S7.

Zanfir-Fortuna, G. (2024). Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package. *Elsevier Analytical Services Research Paper Series*, pp. 01-16.

Zanfir-Fortuna, G. (2024, March 15). Follow the (personal) Data: Positioning Data Protection Law as the Cornerstone of EU's 'Fit for the Digital Age' Legislative Package. *Elsevier Analytical Services Research Paper Series*, pp. 01-16. Retrieved from https://ssrn.com/abstract=4794182 or http://dx.doi.org/10.2139/ssrn.4794182.

*** Court of Justice of the European Union (2021). Case C-340/21: Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021 — VB v Natsionalna agentsia za prihodite. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CN0340.

*** Court of Justice of the European Union (2022). Judgment of the Court (Third Chamber) of 14 December 2023. VX and AT v Gemeinde Ummendorf. Request for a preliminary ruling from the Landgericht Ravensburg. Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Article 82 – Right to compensation and liability – Concept of 'non-material damage' – Online publication of the agenda for a municipal council meeting containing personal data – Publication without the consent of the data subjects – Claim of those data subjects seeking compensation for non-material damage. Case C-456/22. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62022CJ0456.

*** Court of Justice of the European Union (5 December, 2023). Judgments in Cases C-683/21 and C-807/21. Retrieved from https://www.debandt.eu/fr/node/665.

*** Court of Justice of the European Union (2023, January 12). Judgment of the Court (First Chamber) of 12 January 2023. RW v Österreichische Post AG. Request for a preliminary ruling from the Oberster Gerichtshof. Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 15(1)(c) – Data subject's right of access to his or her data – Information about the recipients or categories of recipient to whom the personal data have been or will be disclosed – Restrictions. Case C-154/21. Retrieved from https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62021CJ0154.

*** Court of Justice of the European Union (2023, May 4). Judgment of the Court (Fifth Chamber). In Case C-60/22. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=273289&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4850182.

*** Court of Justice of the European Union (2023, May 4). Judgment of the Court (Third Chamber). In Case C-300/21. Retrieved from https://eu.vlex.com/vid/ui-contro-osterreichische-post-930388280

*** Court of Justice of the European Union (2023, October 23). Reference for a preliminary ruling – Processing of personal data – Regulation (EU) 2016/679 – Articles 12, 15 and 23 – Data subject's right of access to his or her data undergoing processing – Right to obtain a first copy of those data free of charge – Processing of a patient's data by his or her medical practitioner – Medical records – Reasons for the request for access – Use of data for the purpose of triggering the liability of the person providing treatment – Concept of copy. In Case C‑307/22, REQUEST for a preliminary ruling under Article 267 TFEU from the Bundesgerichtshof (Federal Court of Justice, Germany), made by decision of 29 March 2022, received at the Court on 10 May 2022, in the proceedings. Retrieved from https://curia.europa.eu/juris/document/document.jsf?text=&docid=279125&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=3588036.

*** Court of Justice of the European Union (7 March, 2024). JUDGMENT OF THE COURT (Sixth Chamber). Reference for a preliminary ruling – Protection of personal data – Regulation (EU) 2016/679 – Articles 2, 4, 6, 10 and 86 – Data held by a court relating to the criminal convictions of a natural person – Oral disclosure of such data to a commercial company on account of a competition organised by that company – Concept of 'processing of personal data' – National legislation governing access to those data – Reconciliation between the right of public access to official documents and the protection of personal data. https://curia.europa.eu/juris/document/document.jsf?text=&docid=283530&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1.

*** European Commission (2022). Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) (COM/2022/496 final). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496.

*** European Data Protection Supervisor (2024). The History of the General Data Protection Regulation. Retrieved April 27, 2024, from https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

*** European Parliament, Council of the European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

*** European Parliament, Council of the European Union (2022). Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925.

*** European Parliament, Council of the European Union (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065.

*** European Parliament, Council of the European Union (2022). Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2022/868/oj.

*** European Parliament, Council of the European Union (2023). Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2023/2854.

*** European Parliament. EU Artificial Intelligence Act (2024). Retrieved April 26, 2024, from https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf.