New Laws and Regulation

Opportunities for BISE Research

Jella Pfeiffer · Jens F. Lachenmaier · Oliver Hinz · Wil van der Aalst

Published online: 17 October 2024

1 Introduction – The Emergence of a Research Topic

Consider regulations such as the GDPR, the EU AI Act, the Digital Services Act, and the Corporate Sustainability Reporting Directive. In recent years, we as researchers have observed that laws and regulations in the digital domain have rapidly moved to the forefront, raising numerous questions and challenges: Where does the data required to comply with these regulations come from? How can data ecosystems be effectively created and managed, and how can the resulting processes be integrated into information systems? How do users respond when faced with seemingly endless cookie settings? When do users feel they are being treated fairly by AI algorithms?

It appears that a new source of research challenges has emerged alongside our typical research processes: legal and regulatory frameworks. Unlike earlier regulations that focused on specific sectors – such as Basel III or BSBC 239 in the financial industry – these new regulations span multiple sectors at once. In this editorial, we aim to explore the most recent regulations relevant to BISE researchers and outline future research directions. Before delving into specific regulations, we want to emphasize that laws and regulations should be recognized as valuable and intriguing sources of research problems for BISE.

To illustrate this, we begin with a broad perspective by examining a typical BISE research process. This process generally starts with (1) identifying a problem, followed by (2) systematically investigating and studying it, and (3) creating new knowledge and understanding, as well as, sometimes, an artifact. For research to be impactful, the outcomes – whether knowledge or artifacts – should ultimately be (4) transferred into practice (see Fig. 1). While the target audience for BISE is typically understood in the sense of “business” (Benbasat and Zmud 1999), the transfer of research results into the social and political spheres has been the subject of increasing interest. (Weinhardt et al. 2024). There is also the viewpoint that relevance needs to be understood as being pluralistic in nature (Lee et al. 2021; Mohajeri and Leidner 2017), particularly with regards to the diverse range of stakeholders addressed. Indeed, there has been an intense discussion in the BISE community how we can focus not only on rigor, but also on relevance (Österle et al. 2011; Straub and Ang 2011; Buhl et al. 2012). Nunamakar et al. (2015) noted that “going the last research mile means using scientific knowledge and methods to address important unsolved classes of problems for real people with real stakes in the outcome” (Nunamaker et al. 2015, p. 15). Van der Aalst et al. go in a similar direction, calling for open science that makes scientific research and related artifacts accessible to everybody (van der Aalst et al. 2016).

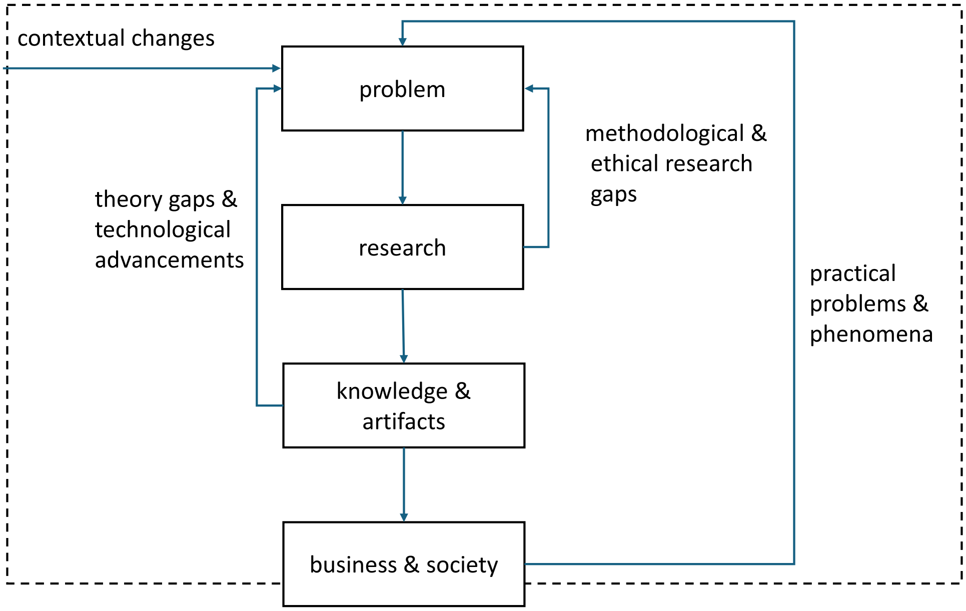
J. Pfeiffer (✉) · J. F. Lachenmaier
Chair of Information Systems 1, Stuttgart University, Keplerstr. 17, 70174 Stuttgart, Germany
e-mail: jella.pfeiffer@bwi.uni-stuttgart.de

J. F. Lachenmaier
e-mail: jens.lachenmaier@bwi.uni-stuttgart.de

O. Hinz
Faculty of Economics and Business Administration, Goethe University Frankfurt, Theodor-W.-Adorno-Platz 4, 60323 Frankfurt am Main, Germany
e-mail: hinz@wiwi-uni-frankfurt.de

W. van der Aalst
Chair of the Process and Data Science group (Lehrstuhl für Informatik 9), RWTH Aachen, Ahornstr. 55, 52056 Aachen, Germany
e-mail: wvdaalst@pads.rwth-aachen.de

Fig. 1 Connections between research steps and problem sources


contextual changes
problem
research
knowledge & artifacts
business & society
theory gaps & technological advancements
methodological & ethical research gaps
practical problems & phenomena

Steps 2 and 3 have also been treated extensively in the literature. All social scientists approach their subject via assumptions about the nature of the world and the way in which it can be studied. This involves assumptions about the ontological (e.g., whether the essence of phenomena is external or the product of individual consciousness) and epistemological nature (e.g., the grounds of knowledge, for example, whether it is hard or soft, or whether it can be acquired or must be personally experienced) (Burrell and Morgan 1979). Burrel and Morgan further consider a third set of assumptions about human nature and its relationship to the environment (e.g., responding in a deterministic way or being in control of and creating the environment). Other authors include axiology, which describes the way we as researchers deal with our own values and those of other people involved in our research (Saunders et al. 2016). The set of assumptions we make as researchers directly influences the methods we choose. There are different ways to categorize these methods. One approach is to distinguish between constructivist, nomothetical and idiographic methods. Constructivist methods focus on the conceptual and technical development of artifacts, as seen in design science (Hevner and Chatterjee 2010; Peffers et al. 2007). Nomothetical methods confirm hypotheses and are often used in BISE by applying surveys and conducting experiments in labs, in the field, or in virtual reality environments (Loomis et al. 1999; Meißner et al. 2019). These methods typically follow the hypothetico-deductive approach. Idiographic methods explore and focus on understanding the unique aspects and complexities of individual cases or events with case studies, action research or ethnography (Baskerville 1999; Iivari et al. 1998). While much more could be discussed regarding the creation of knowledge, artifacts, and research methods, further insights can be found in the works of (Saunders et al. 2016) and (Baskerville et al. 2015).

The driving factor behind the topic of this editorial is step 1 in the research process: Where do the problems we conduct research on originate? We find less research on this important first step and identify several typical sources that are often interrelated rather than mutually exclusive (as illustrated in Fig. 2).

First, our research may be inspired by practical problems and phenomena, typically at the organizational or individual level. Examples include studying the factors that affect the successful transfer to cloud services (Benlian et al. 2018) or how governance and strategic alignment influence organizational performance (Wu et al. 2015). At the individual level, further examples include examining the factors that influence users' trust in e-commerce (Benbasat and Wang 2005) or users' acceptance of large-language-model-based chat interactions in the service industry (Le et al. 2024).

Second, we often seek to identify gaps or inconsistencies in existing theories or research methods. Theory gaps frequently serve a source of inspiration for our research, as theories in BISE can vary widely in nature. They do not only aim at explaining but also focus on analyzing (and describing), predicting, and providing guidance on how to do something (design and analysis) (Gregor 2006). A prominent example is the Unified Theory of Acceptance and Use of Technology (UTAUT; (Venkatesh et al. 2003)), which extended and integrated the Technology Acceptance Model and others by adding several constructs to address theory gaps. Other examples can be found in theory models concerning algorithm aversion, where context-dependent boundary conditions help explain why, in certain situations, algorithms may be appreciated, while rejected in others (Castelo et al. 2019; Heßler et al. 2022). A classic example of a descriptive theory would be Gorry and Scott Morton's framework for Management Information Systems (Gorry and Morton 1989). Besides gaps in theory, there are problems arising from insufficient research methods or ethical concerns (Spiekermann et al. 2022). For example, BISE researchers have intensively discussed and further refined design science as a method (Peffers et al. 2007; Hevner and Chatterjee 2010). Methodological challenges in experimental research for BISE have also been addressed, including optimizing experimental designs (Pfeiffer et al. 2015), and conducting NeuroIS experiments with multiple physiological sensors (Hariharan et al. 2017).

Third, technological advancements often create new opportunities and challenges, prompting research questions about their implications, adoption, and integration. Recent notable examples include advances in AI, such as explainable AI (Bauer et al. 2023) and generative AI (Feuerriegel et al. 2024), as well as virtual and augmented reality (Peukert et al. 2022; Pfeiffer et al. 2020) or blockchain technology (Beck et al. 2017). This third source of research problems highlights the overlap between these sources. For example, with the availability of the latest versions of generative AI tools, concrete problems for companies and users arise, for example concerning privacy and trust. Other technologies, such as the use of blockchain technology for non-fungible tokens in the metaverse, remain more speculative, prompting research questions stemming from potential or prototype implementations. This type of research aligns with the call by Orlikowsky and Iacono to focus more on the IT artifact and to attempt "to understand the complex and fragmented emergence of IT artifacts, [and] how their computational capabilities and cultural meanings become woven in dense and fragile ways […]" (Orlikowski and Iacono 2001, p. 133).

In this article, we highlight a fourth promising source of relevant research questions: contextual changes. These include socio-economic and cultural shifts, such as globalization, financial crises, evolving cultural norms (e.g., polarization, the increasing importance of diversity), as well as phenomena such as pandemics, climate change, and wars. A recent example is research that emerged from the societal, scientific, and educational impacts of the Covid-19 pandemic (van der Aalst et al. 2020). We are particularly also observing the growing prevalence of a subgroup of contextual changes, which is increasingly influencing our research: laws and regulations.

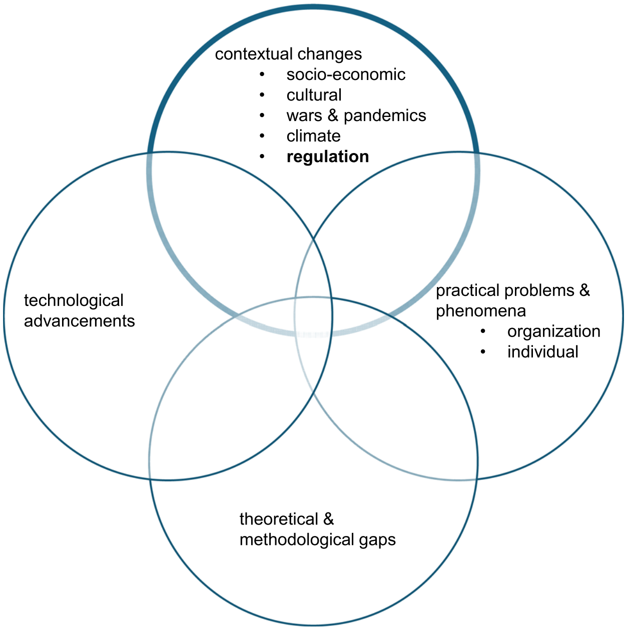


Fig. 2 Problem sources

2 Buckle Up, it's the Law

2.1 Legal Acts in the European Union

As the digital domain continues to grow in value and significance for both businesses and everyday life, it has also attracted increasing public interest and regulatory attention. In response, a rising number of legislative acts have been introduced worldwide to address digital aspects of life and business. Some prominent examples of international laws are the Digital Platform Commission Act of 2023 in the United States, new GDPR-like regulations in individual U.S. states, such as the California Privacy Rights Act and the Utah Consumer Privacy Act, as well as the Cybersecurity Law of the People's Republic of China – to only name a few.

In this article, we are looking at legislation by the European Union (EU) that affects us as the BISE community. We have chosen the EU because, with GDPR and the EU AI Act, we have two prominent examples with which the EU seems to be the pioneer with important regulations concerning digital business. The EU's overarching goal is to establish a single, common market for all its members, encompassing both digital and physical markets. This goal also applies to international companies that wish to provide products and services within the EU. The legislative process in the EU involves several key bodies: the European Parliament, the Council of the EU, and the European Commission. These institutions work together to create new laws, referred to as legal acts. We will focus on the binding types of legal acts, which include:

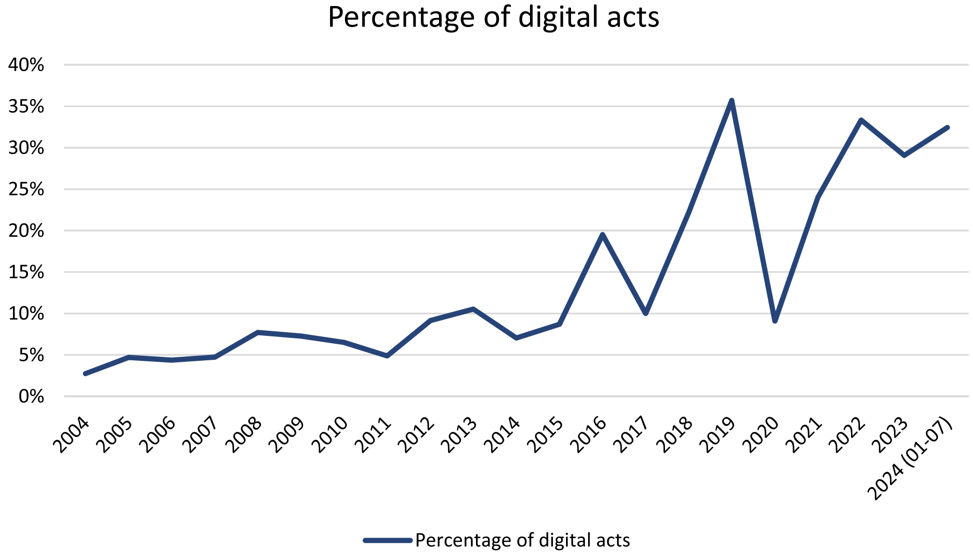


Fig. 3 Percentage of legal acts concerning digital topics compared to all legal acts passed by the EU per year *Source*: EUR Lex.

- Regulations, that are directly binding for all member states,
- Directives, which set goals that must be achieved by national law,
- Decisions, which are often addressed to a specific target group or one state.

The more extensive laws are regulations and directives. Over the last 20 years, the EU has passed 7728 new regulations and directives (see Fig. 3). While the pace of lawmaking may be slowing due to the increasing complexity of legislative processes, efforts for "better regulation" (European Commission 2024b), and ongoing amendments to existing laws, this trend does not hold true for the digital domain. In 2021, the EU declared the onset of the "digital decade", setting the ambitious goal of creating "a human-centered, sustainable and more prosperous digital future" (European Commission 2024c). This vision is to be realized through a series of regulations and funding measures that help to convey skills, empower the government, improve infrastructures and gear up business for the digital transformation (European Union 2024). This has so far resulted in about 75 new legal acts since 2021 and leads to an increasing share of acts that address the digital domain[1]. Details on the progress of the digital decade can be found in the track record published by the EU (European Commission 2024a).

BISE, however, is not only concerned with legislation aimed at the digital domain; it also addresses other significant legal acts that have been passed in recent years that have direct or indirect ramifications on BISE related topics. For example, acts that deal with the supply chain or with corporate social responsibility may require the development of corresponding information systems to monitor or report relevant issues. Table 1 provides a selective overview of acts that might be of interest for BISE researchers. We have selected them based on their connection to BISE as well as their timeliness and have grouped them by the topic they address.

To further examine these legal acts from a BISE perspective[2], we clustered them into four groups, while acts that belong into more than one groups are possible, (see also last column of Table 1): (1) data interoperability, sharing, and protection, (2) specific technologies, (3) digital markets and services, and (4) cyber security.

Acts on data interoperability, sharing, and protection: Many legal acts concern data which focus on one of three areas: First, acts that govern data collection and data sharing. Data collection and data sharing are essential to achieve transparency, for example in supply chains. Data is the foundation for any type of reporting, and as such, must be carefully managed to comply with legal requirements set by laws such as the Corporate Sustainability Due Diligence Directive and the Corporate Sustainability Reporting Directive. Second, there are acts specifically addressing data provision to authorities, such as Digital Identity frameworks or public Open Data initiatives. Third: there are acts related to data sharing. These acts deal with data sharing across company borders and specifically address industrial IoT data. This is meant to foster new

[1] An act is considered to concern the digital domain when it addresses either the theme of "information technology and data processing" or one of the subcategories of "information" (selected subcategories are: information system, exchange of information, data sharing, data protection, data governance, open data, artificial intelligence) in the EU Lex database.

[2] For further details on the legal perspective, we recommend the work of Aueamnuay et al. who assessed the legal quality and impact of various digital acts passed by the EU (Aueamnuay et al. 2024).

Table 1 Selected digital acts by the EU that matter in BISE

Year	Legal act	Purpose [quotes from official EU documents]	Group
Group 1: data interoperability, sharing, and protection			
2018	General data protection regulation (GDPR)	Protection of personal data Free movement of personal data within the Union	1
2018	Regulation on the free flow of non-personal data	Removing obstacles to the free movement of non-personal data between different EU countries and IT systems in Europe	1
2018	Single digital gateway	Facilitates online access to information, administrative procedures, and assistance services that EU citizens and businesses may need in another EU country	1
2019	Directive on open data and the re-use of public sector information	legal framework for the reuse of public-sector information such as geographical, land registry, statistical or legal information held by public-sector bodies or public undertakings, and of publicly funded research data	1
2022	Data governance act	Increase trust in data sharing Strengthen mechanisms to increase data availability Overcome technical obstacles to the reuse of data	1
2023	Corporate sustainability due diligence directive (CSDDD)	Foster sustainable and responsible corporate behavior in companies' operations and across their global value chains	1
2023	Corporate sustainability reporting directive (CSRD)	Modernize and strengthen the rules concerning the social and environmental information that companies have to report	1
2024	Data act	Making data (in particular industrial data) more accessible and usable Encouraging data-driven innovation Increasing data availability	1
2024	European digital identity (eudi) regulation	Enable the creation of a universal, trustworthy, and secure European digital identity wallet	1
2024	European health data space regulation	Empower individuals to take control of their health data and facilitate the exchange of data for the delivery of healthcare across the EU Foster a genuine single market for electronic health record systems Provide a consistent, trustworthy, and efficient system for reusing health data for research, innovation, policy-making, and regulatory activities	1
2024	Interoperable Europe act	Facilitate cross-border data exchange Accelerate the digital transformation of the public sector	1
Group 2: Acts on specific technologies			
2022	Pilot regime for market infrastructures based on distributed ledger technology	Remove regulatory barriers to the issuing, trading and settlement of crypto-assets that are financial instruments	2, 3
2024	AI act	Address risks to health, safety and fundamental rights Protect democracy, rule of law and the environment	2
Group 3: Acts on the digital market			
2022	Digital markets act	Make the markets in the digital sector fairer and more contestable	3
2022	Digital services act	Prevent illegal and harmful activities online Prevent the spread of disinformation	3
2022	Pilot regime for market infrastructures based on distributed ledger technology	Remove regulatory barriers to the issuing, trading and settlement of crypto-assets that are financial instruments	2,3
Group 4: Acts on cyber security			
2016	Network and information systems directive 1 (NIS 1)	Improved cybersecurity capabilities at the national level Increased EU-level cooperation Risk management and incident reporting obligations for operators of essential services and digital service providers	4
2022	Network and information systems directive 2 (NIS 2)	Improve the resilience and incident response capacities of public and private entities, competent authorities and the EU	4
Upcoming	Cyber resilience act	Safeguard consumers and businesses buying or using products or software with a digital component	4
Upcoming	Cyber solidarity act	Strengthen common EU detection, situational awareness, and response capabilities, Build an EU-level cybersecurity reserve with services from trusted private providers, and Support testing of critical entities	4

digital business models to strengthen the competitiveness of European companies. Relevant acts are the Data Governance Act, the Data Act, and the Health Data Space Regulation. Lastly, this group also includes the General Data Protection Regulation (GDPR), which is well-established and focuses on the protection of personal data.

Acts on specific technologies: The EU tries to regulate impactful technologies, such as blockchain and AI. With the first AI regulation worldwide and the pilot market for blockchain applications in the financial sector, the EU considers itself to be on the forefront of digital legislation. The pilot market regulation for distributed ledger technology creates temporary exempts from existing other legal requirements in the financial industry. The purpose of this act is to give financial institutions the possibility to advance their business models and authorities to gain practical insights into the application and control of blockchain technologies. The AI Act aims to provide a comprehensive legal framework for AI developers, outlining the requirements for AI systems used within the European Union. It classifies AI applications into four risk categories: unacceptable, high, limited, and minimal risk. For high-risk AI systems, the Act imposes stricter obligations. These are systems that are used as safety components in critical infrastructure, profile individuals, or determine access to educational institutions or for recruitment of companies. Providers of such systems must implement risk management and quality management systems, ensure thorough documentation, and maintain human oversight in decision-making processes to ensure that humans-in-the-loop retain the final authority in key decisions.

Acts on the digital market: With the increasing market share of global hyperscaling platforms and the growing significance of social media, the EU has introduced rules specifically targeting these providers to ensure the safe, secure, and efficient use of their digital services. At the same time, these regulations aim to reduce the influence of platforms as gatekeepers. Since platforms have the ability to steer users towards certain websites or withhold others, the Digital Markets Act (DMA) ensures equal rights for all market participants, prohibiting platforms from prioritizing their own products and services. These laws are particularly focused on protecting users' rights by regulating platform providers and shielding users from illegal or misleading content. The Digital Services Act (DSA), for instance, targets the largest platforms, specifically those with at least 45 million users in Europe. Non-compliance with these acts can result in significant penalties, with companies facing substantial fines for failing to adhere to the regulations.

Acts on cyber security: Cybersecurity has become a major focus in European legislation, with numerous acts passed since 2018 and more expected in the near future. The organization "Interface" has identified 154 legal acts related to cybersecurity (Rupp 2024). As digital services are now the foundation of modern society and everyday life, the EU is making efforts to ensure that critical infrastructure, in particular, is well-protected against cyber threats. These regulations cover a wide range of areas, from ensuring a more secure global Internet and establishing rules for secure digital products, to forming joint defense centers that integrate cyber defense capabilities. The legislation also includes industry-specific regulations targeting sectors such as energy, finance, transportation, and education. A key principle in these regulations is the risk-based approach, which requires organizations to identify potential risks and implement measures to mitigate them (Lemnitzer 2022). Additionally, companies are obligated to report cyber-attacks, and they can be audited for their preventive measures. In the worst-case scenario, failure to pass an audit could result in a company's operations being halted, and corporate leaders may be held personally liable for their organization's cybersecurity posture.

2.2 Existing Research on Laws and Regulations

So, how exactly have researchers in the BISE community addressed these new laws and regulations in the past? We have identified several contributions that fall into three key areas:

a) Investigating specific regulations, particularly for their impact on the BISE domain
b) Designing new solutions to handle challenges arising from legislation
c) Discussing the contribution of BISE to legislation in general.

Research focusing on legal acts (A): In recent years, research has also examined the impact of specific regulations on research: Vainionpää et al. (2023) conducted a deep dive into the AI Act. After presenting and discussing potential challenges, they proposed a research agenda for further research based on the AI Act. They analyzed the scope of the AI Act, as well as its approach, wording, coherence with other laws, and enforcement. From this analysis, they identified three key areas for future research: the daily handling of the regulation within organizations, the law itself, and its long-term effects.

Similarly, Pfeiffer et al. (2023) explored algorithmic fairness as a critical aspect of the EU AI Act. Their discussion in the BISE community covered topics such as the definition of fairness, the mitigation of bias and discrimination in AI systems, and the long-term impacts of AI with respect to its trustworthiness. Empirical studies such as the one by Bauer et al. (2024) investigated how machine learning impacts human discrimination and how these findings relate to the AI Act. Their papers also analyzed the effects of explainable AI, which is explicitly demanded by the AI Act, on the mental processes of decision makers and highlight some potential, unwanted downstream consequences of these regulations (Bauer et al. 2023).

Regarding the Digital Markets Act, Weigl et al. (2023) examined its implications for privacy, while Shekhar et al. (2022) focused on its economic effects. Weigl et al. (2023) showed that the goal of data sharing – which is necessary to allow more players to compete in the digital realm – may be in conflict with the GDPR and, thus, developed a recommended procedure based on the type of anonymization that is possible in a given situation. Shekhar et al. (2022) found that the mandated compatibility between platforms will lead to reduced platform profits but to an increase in total welfare, including developers and consumers.

Additionally, some researchers, such as Heimburg et al. (2023) have investigated the law-making process itself. By gathering and analyzing public comments made during the drafting of regulations, they determined impacts on issues such as power distribution and value creation, which in turn are to be considered in platform-based ecosystems.

Research addressing challenges arising from legislation (B): Design-oriented research has already begun addressing the requirements stemming from new laws and regulations. One example that is broadly discussed in the literature is the proposal of blockchain data storage for supply chains, with the goal of creating a sophisticated level of documentation, which can be trusted by all parties, including auditors (Kumar et al. 2020; Chandan et al. 2019). Blockchain can also be used to document greenhouse gas emissions (Darwish et al. 2023). Other circular economy data can be stored in a digital twin as suggested by Monteiro and Barata (2024).

There is existing research about the design of GDPR-compliant information systems (Guggenmos et al. 2020) as well as cybersecurity-compliant systems – in this example in the healthcare domain (Plachkinova and Faddoul 2022). Additionally, information systems are being explored as tools for reducing Scope 3 greenhouse gas emissions within organizations, though several challenges remain (Cauderay et al. 2024).

Further, researchers have looked into the strategic integration of the Corporate Sustainability Reporting Directive (CSRD) into corporate management systems. For instance, decision support systems have been highlighted as crucial for achieving sustainability goals (Farkas and Matolay 2024). The study by (Krasikov and Legner 2023) outlines how companies are developing specialized data procurement practices to ensure reliable sustainability reporting.

Articles focusing on the influence of BISE on legislation (C): As described in the introduction, the transfer of research outcomes to the society is an essential part of the research process. This makes it crucial to engage with policymakers and political actors, informing them of relevant research findings that could influence their decision-making.

The discussion on how to establish a continuous exchange between the BISE community and the political domain has been ongoing for quite some time. For example, as early as 1997, an ICIS panel discussed the intersections between politics and information technology (Romm et al. 1997). Later, Beck called on researchers to become more involved in politics and to develop a political agenda (Beck 2002). This conversation continued with panel discussions in 2012 and 2019, where international BISE researchers shared arguments, opinions, and recommendations (Loebbecke et al. 2012; Fedorowicz et al. 2019). More recently, Weinhardt et al. (2024) published an editorial proposing a research agenda on digital democracy, highlighting IT regulation as a key area of focus. Their article emphasizes the need to enhance public understanding of technological and digital innovations. The authors argue that it is the duty of information systems researchers to provide the public with the necessary tools, guidance, and education. We support this call to action, stressing the importance of well-informed lawmaking to minimize unintended consequences and maximize the benefits of digital advancements.

3 Research Topics that Arise from Regulation

In our view, there are numerous research topics open for further exploration. Therefore, we propose a range of research topics and questions to inspire BISE researchers. Table 2 presents one legal act from each of the groups discussed earlier, along with corresponding research topics. These topics are listed in no particular order, and some are further elaborated below. While the list is not exhaustive, it is intended to serve as a foundation to encourage BISE researchers to pursue these relevant and timely areas of inquiry.

Research topics arising from the Data Act: Data sharing will soon become mandatory for specific industries and data sources to maximize the value of data and reduce redundant data collection. But in order to achieve those benefits of data sharing, we need to overcome different hurdles on the way.

Even though the potential benefits for better analytic results based on a more extensive data basis and the possibility of leveraging third party analytic capabilities and resources are promising – especially to SMEs, currently, many companies are reluctant to share data with others. To address this, a framework should be developed that helps organizations assess the criticality and importance of their

Table 2 Research topics based on legal acts

Group: selected legal act	Research topics
Data interoperability, sharing, and protection: data act	Which framework could guide companies regarding the criticality and value of data?
	How can data trustees facilitate data sharing between organizations?
	How can we design, implement and promote data spaces and data ecosystems that foster inter-organizational data sharing?
	Which data is truly necessary to achieve desired outcomes?
	How can we verify or validate the quality and trustworthiness of external data that has been shared by third parties?
	What prevents companies from implementing privacy-by-design paradigms?
	How can effective and efficient processes be designed to handle user privacy requests?
	How can we effectively separate shared data from sensitive data (e. g. due containing to personal data or business secrets)?
	How can we manage new outsourcing and cloud models, such as Compute-as-a-Service, that leverage offshore development or are intended to reduce the amount of involved personal data?
Technologies: AI act	How to assess whether an application falls under the AI definition of the EU AI Act?
	Which framework can we establish to help categorize AI applications into appropriate risk classes?
	How can the sandbox concept of the EU AI Act be implemented in a way that encourages SMEs to invest in AI development?
	What specific challenges does the AI Act pose to existing AI governance and strategy frameworks and how can we reconcile those frameworks with the AI act?
	How should an effective market for third-party certification of AI systems be designed?
	Which measurements and processes are necessary to certify compliance with the EU AI Act?
	What are user perceptions of fairness, and how can we mitigate discrimination in AI systems?
Digital market and services: digital service act	How can we efficiently detect and flag incorrect information, hate speech and other illegal content?
	How can we identify and mitigate harmful network effects and power dynamics? How can we generate, govern, and foster beneficial ones?
	How can we design effective structures for the handling of such content?
	How can we leverage gamification to stimulate user participation?
	What is the impact of removing undesired content on different user groups and their internet usage patterns?
	How is the Digital Services Act affecting the ecosystem surrounding platform providers?
Cyber security: network and information systems directive 2	Which are the critical factors that determine an organizations' level of security?
	How can we design information systems that follow the paradigms of security by design or zero trust?
	What are possible frameworks for risk management and risk assessment?
	Which processes and structures enable organizations to handle cyber-attacks efficiently and effectively?
	How can we leverage the potential of new technologies while addressing cybersecurity challenges?
	How can we systematically learn from incidents, share experiences across organizations and prevent future occurrences?
	How can the coordination of government agencies be improved from an e-government perspective?
Research topics that concern all the groups at once	What are the benefits, tasks, and required skills and tools for the new role of a Chief Regulation Officer?
	How can we turn the adherence to regulations into a competitive advantage?
	What mechanisms can be established to facilitate ongoing communication between lawmakers and the BISE community to keep them informed about critical topics?
	How can we handle different legal requirements in different countries in information systems?
	How can automated tools for documentation purposes be designed?
	How to predict and weigh intended versus unintended consequences that arise from new laws?
	How can we incorporate laws and regulations in the BISE community and into teaching?
	Why and how do local implementations of directives differ across EU member states?
	Why are legislators creating specific regulations, and do these achieve the desired outcomes?
	How are the regulations impacting start-ups?

data sets in relation to their specific business models. This framework would guide companies in identifying which data can be shared without negatively impacting their operations. Additionally, companies must weigh the potential benefits of data sharing against the associated risks, making decisions about whether to share data with partners or the public. The framework should, therefore, consider criteria that determine the risk of data sharing versus its benefits. One method to differentiate between critical and non-critical data is by separating data from its context, as suggested by Werling et al. (2022). Once the decision to share data has been made, the question arises: how should this data be shared? One current model involves data brokers or data trustees who manage data exchanges. However, the definition, roles, and obligations of data trustees are still under development, and their authority or ability to intervene in case of issues has not yet been finalized. The data trustees can run so-called data spaces that are the infrastructure for data management. Hutterer states that even though the idea of data spaces is very promising, it is impossible to get empirical insights into their mechanisms due to the lack of implemented data spaces (Hutterer 2023).

On the other hand, before using external data which we have received in critical applications, both users and developers need to be sure that the external data is accurate, correct, and reliable. This has so far been discussed as an issue of data quality, which is typically addressed within one organization. Most of the time, the organization that produces the data has a good understanding of its data quality – but others will not because they do not know how the data was generated. We therefore propose to look at the data quality problem from another perspective, which is: how can we verify or validate external data to assess its data quality? We need to develop mechanisms and procedures that can help with the task of assessing the quality of data collected by others. Mechanisms to address this could include comparing data with other sources, involving or creating trusted third-parties to assess and certify data quality (Baars et al. 2022; Weber et al. 2023), or detecting outliers by comparing the data to expected or standard operational values.

Research topics arising from the AI Act: The EU AI Act has been under discussion for five years across various European boards and countries and has evolved into an extensive piece of legislation. One of the main challenges is the dynamic evolvement of AI. For example, generative AI was hardly part of the first draft of the EU Act but needed to be incorporated during the development of the regulation (see, for instance, recitals 99 and 105 of the EU AI Act). Likewise, other aspects in the AI Act are formulated quite openly and leave room for further discussion and development, like the definition of AI itself or the assignment of AI applications to risk classes. Companies face the challenge of judging which of the applications fall under the Act's AI definition and if so, whether they belong to the high-risk class. This classification is particularly challenging and context dependent. For example, determining whether an AI application used in critical infrastructure management or digital infrastructure should be classified as high-risk requires careful consideration of its operational context. Here, BISE research can provide valuable insights by helping to assess AI applications within specific business or safety frameworks. BISE research, such as research on NeuroIS, may even be impacted by the AI Act itself, especially if the systems are designed to detect emotions in educational or workplace environments. The AI Act adopts a broad definition of "emotion," extending to user intentions and feelings such as satisfaction. This raises questions on how the used definitions in the AI Act fit to our understanding of long and well-studied concepts in research. Although the AI Act explicitly does not apply to AI systems and models "specifically developed and put into service for the sole purpose of scientific research and development" (see recital 6 EU AI Act), the regulation may still influence funding efforts. This is because AI models initially developed for scientific research may later be adapted for commercial purposes and put on the market. Consequently, funding bodies may require research projects to consider compliance with the broader regulatory framework, anticipating the potential future commercialization of these models.

Another interesting area of research comes from the obligation for certification and compliance with the AI Act. There is a need to develop processes and measurements that help companies to check for compliance need to be developed. This is a core area of expertise for BISE researchers. However, compliance involves not only monitoring and control but also a comprehensive approach to AI strategy and governance. For high-risk AI systems, organizations must implement a quality management system that includes a clear strategy for regulatory compliance. Additionally, the AI Act mandates a risk management system throughout the life cycle of a high-risk AI system, covering mitigation and control measures. BISE researchers that have a tradition in IT management, strategy and governance are well-positioned to explore the specific challenges that the AI act poses to existing theories and frameworks. This includes identifying the roles and responsibilities needed for managing critical AI applications, decision-making processes for AI development, and strategies for keeping AI systems up to date and in compliance. Finally, the EU AI Act is expected to impact the society as a whole and in the long-term. For example, algorithmic discrimination might manifest itself because the same software is used for many different decisions, and it might be self-reinforcing because decisions made by AI algorithms are used for re-training and fine-tuning (Pfeiffer et al. 2023). The AI Act seeks to acknowledge these threats and stresses the fact that AI algorithms must not discriminate, a principle already enshrined in EU law. Thus, BISE researchers are asked to investigate how to mitigate algorithmic discrimination and how to ensure that all users are treated equally.

Research topics arising from the Digital Service Act: The Digital Services Act (DSA) requires platform providers to detect and remove illegal content, such as hate speech and misinformation, offering significant opportunities for researchers to improve methods for identifying problematic content. Sentiment analysis is one of the core technologies addressing this challenge by interpreting subjective information such as sentiments, opinions, and emotions in user-generated content (Ligthart et al. 2021; Nandwani and Verma 2021). Techniques in sentiment analysis range from lexicon-based methods, which use predefined word lists to assess sentiment, to machine learning-based approaches, such as supervised and unsupervised learning, which train models to classify sentiments. Deep learning-based approaches, including CNNs, LSTMs, and transformers, have significantly enhanced sentiment detection by automatically learning intricate patterns from large datasets. Transformers, such as BERT and DistilBERT, are particularly relevant due to their ability to capture long-range dependencies and contextual meanings in text, offering more accurate sentiment analysis, especially in complex cases, but also requiring substantial computational resources (Acheampong et al. 2021). Researchers can continue to refine these models to detect more subtle forms of problematic language, such as sarcasm or implicit hate speech, or explore hybrid approaches that combine the strengths of lexicon-based, machine learning, and deep learning techniques. Additionally, engaging users in content moderation through gamification or nudging mechanisms can encourage participation, enhancing both user engagement and the platform's ability to manage content effectively.

The Digital Services Act (DSA) also mandates that providers of intermediary services publish detailed reports on their content moderation practices. These reports must include data on the number of content removals and the accuracy rates of their automated content moderation systems. To ensure this information is both accessible and transparent to users, there is a growing need to research effective designs for conveying these metrics. Clear and intuitive designs will help users understand how content is managed on these platforms and promote trust in the system.

Beyond the central platform, a broader ecosystem of partners – including content creators, advertisers, and service providers – often operates within the platform's structure. The impact of the DSA on this ecosystem has not yet been thoroughly explored, raising important questions about how these partners are affected by the regulation. Researchers can investigate how the new reporting requirements and content moderation processes influence not only the platform but also its connected stakeholders, potentially uncovering challenges or opportunities for adaptation within this ecosystem.

Research topics arising from Network and Information Systems Directive 2: As many more companies and organizations are now considered to be part of the critical infrastructure than before, these affected organizations need consulting and guidance on assessing their security maturity and prioritizing cyber defense measures. Most of these companies are SMEs, which means that they suffer from a lack of resources. They need clear priorities on how to approach the topic of cyber security, how to do a risk assessment, and how to act to ensure the security – and as a logical consequence also the safety – of their operations. Therefore, maturity models and frameworks or guidelines are needed that can help to determine the current status and outline a clear path to getting more secure. Surveys that cover questions from which the current level of security can be deduced are one possible approach here.

The same holds true for auditors who have the task of assessing the level of security in a given company. The process of auditing is cumbersome and is handled different by each individual auditor. Based on personal experience and expertise, an auditor can make exceptions to defined security requirements. Streamlined auditing processes will become increasingly important as the number of companies requiring audits grows due to the expanded definition of critical infrastructure. When a cyberattack occurs, organizations must quickly mobilize their cyber defense capabilities. This requires well-defined roles, systems, and processes to manage threats efficiently. Developing a robust incident reporting mechanism is key to a successful defense. BISE researchers can contribute by leveraging their experience from enterprise architecture management, offering guidance on how to come up with new capabilities, and providing the enterprise architecture information necessary to assess the impact of an attack. For smaller organizations, outsourcing certain cyber defense functions to specialized partners may also be a viable option, highlighting the importance of effective partner management in this context. The relationship between AI and cyber security is twofold and there have been publications about both directions – AI can be a new threat, for example when it is asked to program a new encryption virus, and AI can be used to protect against cyber threats, for example when AI is used to detect unusual network traffic (Becklines 2024; Shanbhag et al. 2024; Sinha and Muktevi 2024). As a result, companies have to be on the lookout for new challenges to their cyber security as well as their technical defenses continuously, and could be supported by automated mechanisms that inform them about current developments. One research topic could be to identify relevant information demand to keep informed about ongoing developments and suitable sources to cover the demand. Dashboards could be designed based on this information to display threat levels can help security experts manage risks more effectively. Another related research topic might be how to provide the most effective security training to employees, as the continuous education of employees will be increasingly important in safeguarding organizations.

Research topics arising from the complete set of new regulations: Analyzing the law-making process is crucial for improving the efficiency of future legislation, enabling timelier implementation of necessary changes. Here, we could apply process mining to determine bottlenecks or unstructured parts in the processes. One example of such a project that provides access into the engine room of German legislation is Open Discourse (Richter et al. 2020), which is providing the data foundation for analytics regarding the progress of law-making and regarding the political debate. Besides Open Discourse, which relies on protocols from debates, it would also be possible to collect statements from different interest groups and see how the draft of a law is changing over time to reflect demands by specific groups. An example is the transparently documented progress of the German NIS 2 implementation as published by the state (Bundesministerium des Inneren und für Heimat 2024). Such a document analysis involving multiple European member states could also help to answer the question of why and how the implementations of directives are different from each other in each member state.

In addition, the general use of tools, especially generative AI-based tools, which could either help identifying problematic or contracting regulations during the process or legislation, or help documenting how the legal requirements are addressed by the individual company, should be leveraged. Top-down, generative AI can be used to write a template for a company's cyber security policy but must then be fitted to the individual company and needs to be binding for all parts of the company. Bottom-up, we can use tools to document the IT landscape and the business architecture or tools for penetration testing to identify vulnerable parts of the infrastructure.

The increasing number of regulations has to be handled on the company level. This is especially important when operating in an international context, which requires adherence to even more laws than the ones discussed so far. Furthermore, with the growing severity of penalties for non-compliance, the financial and operational impact on organizations can be significant. Some companies have already started to implement Chief Regulation Officers that monitor laws and regulations and try to intervene when new laws emerge. As with other CxOs, their roles, responsibilities, and impact should be evaluated. Other forms of institutionalization include competence centers within companies or specialized consulting services that could be offered by industry associations.

In any case, we need to educate more people on these topics due to their relevance and impact on multiple job profiles, such as security consultants and data scientists. The law-making process and opportunities to influence these processes should be incorporated into the study programs of BISE students. Conversely, we should also aim to educate law students on BISE-related topics. To achieve the best outcomes, collaboration with legal specialists is essential. Additionally, we should strengthen the connections between BISE researchers and legislators to contribute our insights on these critical topics that have extensive consequences.

These consequences are sometimes unintended as we have seen with the browser cookies based on GDPR (Johnson et al. 2023). To avoid such issues in the future, BISE researchers are asked to develop methods to predict these unintended consequences. This could be achieved – at least in some cases – by involving experts from the BISE community in the legislative process. Also, to further reduce unintended consequences and to ensure compliance of digital products and services with current laws, third parties that inspect and certify products could be involved.

Finally, we could investigate how companies subject to new laws are performing in comparison to companies operating outside of the EU. Can they leverage the potential benefits of regulations, or are these regulations hampering innovation? This may become apparent when we consider start-ups and their chances of success, which are influenced by the balance between innovation potential and regulatory barriers, such as the administrative overhead they must address. The same is true at the societal level – how are political debates progressing in regions that embrace measures against misinformation compared to those that do not, and how is technology usage and acceptance impacted by the regulations?

These new regulations provide diverse and exciting opportunities for BISE research. We are eager to see developments in the coming years and recommend initiating the respective research projects now to assess the impact of these regulations before they come into full effect. Based on these insights, we can in turn become even more valuable partners to legislators and policymakers in broadening the impact of BISE research and developing effective regulations that strengthen our businesses, and improve the cohesion of our society.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Acheampong FA, Nunoo-Mensah H, Chen W (2021) Transformer models for text-based emotion detection: a review of BERT-based approaches. Artif Intell Rev 54(8):5789–5829. https://doi.org/10.1007/s10462-021-09958-2

Aueamnuay C, Berjón C, Galehr S, Graf L, Heinemann A (2024) Digital regulation in the European Union. EuZ Z Europarecht. https://doi.org/10.36862/eiz-euz2024-03

Baars H, Weber P, Tank A (2022) Institutionalizing analytic data sharing in SME ecosystems – A role-based perspective. In: HICSS Proceedings, pp. 6135–6144 http://hdl.handle.net/10125/80084

Baskerville RL, Kaul M, Storey VC (2015) Genres of inquiry in design-science research. MISQ 39(3):541–564

Baskerville RL (1999) Investigating information systems with action research. Commun Assoc Inf Syst. https://doi.org/10.17705/1CAIS.00219

Bauer K, von Zahn M, Hinz O (2023) Expl (AI) ned: the impact of explainable artificial intelligence on users' information processing. Inf Syst Res 34(4):1582–1602. https://doi.org/10.1287/isre.2023.1199

Bauer K, Heigl R, Hinz O, Kosfeld M (2024) Feedback loops in machine learning: a study on the interplay of continuous updating and human discrimination. J Assoc Inf Syst 25(4):804–866. https://doi.org/10.17705/1jais.00853

Beck EE (2002) P for political: participation is not enough. Scand J Inf Syst 14(1):77–92

Beck R, Avital M, Rossi M, Thatcher JB (2017) Blockchain technology in business and information systems research. Bus Inf Syst Eng 59(6):381–384. https://doi.org/10.1007/s12599-017-0505-1

Becklines L (2024) FAIDS: artificial intelligence developmental systems framework for predicting and preventing cyberattacks in supply chain networks. In: AMCIS Proceedings, Salt Lake City

Benbasat I, Wang W (2005) Trust in and adoption of online recommendation agents. J Assoc Inf Syst 6(3):72–101. https://doi.org/10.17705/1jais.00065

Benbasat I, Zmud RW (1999) Empirical research in information systems: the practice of relevance. MISQ 23(1):3–16. https://doi.org/10.2307/249403

Benlian A, Kettinger WJ, Sunyaev A, Winkler TJ (2018) Special section: the transformative value of cloud computing: a decoupling, platformization, and recombination theoretical framework. J Manag Inf Syst 35(3):719–739. https://doi.org/10.1080/07421222.2018.1481634

Buhl HU, Fridgen G, Müller G, Röglinger M (2012) On dinosaurs, measurement ideologists, separatists, and happy souls: proposing and justifying a way to make the global IS/BISE community happy. Bus Inf Syst Eng 4(6):307–315. https://doi.org/10.1007/s12599-012-0239-z

Bundesministerium des Inneren und für Heimat (2024) Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung. https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html. Accessed 17.09.2024

Burrell G, Morgan G (1979) Sociological paradigms and organisational analysis – elements of the sociology of corporate life. Ashgate, Hants

Castelo N, Bos MW, Lehmann DR (2019) Task-dependent algorithm aversion. J Mark Res 56(5):809–825. https://doi.org/10.1177/0022243719851788

Cauderay V, Haskamp T, Sebastian IM, Uebernickel F (2024) Talking about the elephant in the room: Findings from a literature review on leveraging information systems for reducing scope 3 emissions. In: ECIS Proceedings, Paphos

Chandan A, Potdar V, Rosano M (2019) How blockchain can help in supply chain sustainability. In: ACIS Proceedings, Perth, pp. 953–960

Darwish A, Lindman J, Hjertqvist J, Tona O (2023) Design principles for blockchain-based applications in green bond reporting. In: HICSS Proceedings, Lahaina, pp. 5186–5195

European Commission (2024a) 2030 Digital decade - Annex 1. https://doi.org/10.2759/635

European Commission (2024b) Better regulation: why and how. https://commission.europa.eu/law/law-making-process/planning-and-proposing-law/better-regulation_en. Accessed 17 Sep 2024

European Commission (2024c) Europe's Digital Decade: digital targets for 2030. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en. Accessed 17 Sep 2024

Farkas M, Matolay R (2024) Designing the CSRD system: insights from management systems to advance a strategic approach. J Decis Syst. https://doi.org/10.1080/12460125.2024.2354614

Fedorowicz J, Bjørn-Andersen N, Olbrich S, Tarafdar M, Te'eni D (2019) Politics and AIS: where do we draw the line? Commun Assoc Inf Syst 44(1):247–261. https://doi.org/10.17705/1CAIS.04416

Feuerriegel S, Hartmann J, Janiesch C, Zschech P (2024) Generative AI. Bus Inf Syst Eng 66(1):111–126. https://doi.org/10.1007/s12599-023-00834-7

Gorry GA, Morton MSS (1989) A framework for management information systems. MIT Sloan Manag Rev 30(3):49–61

Gregor S (2006) The nature of theory in information systems. MIS Q 30(3):611–642

Guggenmos F, Lockl J, Rieger A, Wenninger A, Fridgen G (2020) How to develop a GDPR-compliant blockchain solution for cross-organizational workflow management: evidence from the German asylum procedure. In: HICSS Proceedings, Wailea, pp. 4023–4032

Hariharan A, Adam MT, Dorner V, Lux E, Mueller MB, Pfeiffer J, Weinhardt C (2017) Brownie: a platform for conducting NeuroIS experiments. J Assoc Inf Syst 18(4):264–296. https://doi.org/10.17705/1jais.00457

Heimburg V, Schmitt J, Wiesche M (2023) The future of digital platform design – The case of the EU platform regulation discourse. In: ECIS Proceedings, Kristiansand

Heßler PO, Pfeiffer J, Hafenbrädl S (2022) When self-humanization leads to algorithm aversion: what users want from decision support systems on prosocial microlending platforms. Bus Inf Syst Eng 64(3):275–292. https://doi.org/10.1007/s12599-022-00754-y

Hevner A, Chatterjee S (2010) Design research in information systems: theory and practice. Springer US, Boston, MA

Hutterer A (2023) Introduction of data spaces – status and recommendations for action. In: ICEB Proceedings, Chiayi, pp. 377–390

Iivari J, Hirschheim R, Klein HK (1998) A paradigmatic analysis contrasting information systems development approaches and methodologies. Inf Syst Res 9(2):164–193. https://doi.org/10.1287/isre.9.2.164

Johnson GA, Shriver SK, Goldberg SG (2023) Privacy and market concentration: intended and unintended consequences of the GDPR. Manag Sci 69(10):5695–5721. https://doi.org/10.1287/mnsc.2023.4709

Krasikov P, Legner C (2023) Introducing a data perspective to sustainability: how companies develop data sourcing practices for sustainability initiatives. Commun Assoc Inf Syst 53(1):162–188. https://doi.org/10.17705/1CAIS.05307

Kumar A, Liu R, Shan Z (2020) Is blockchain a silver bullet for supply chain management? Technical challenges and research opportunities. Decis Sci 51(1):8–37. https://doi.org/10.1111/deci.12396

Le KB, Sajtos L, Kunz WH, Fernandez KV (2024) The future of work: understanding the effectiveness of collaboration between human and digital employees in service. J Service Res. https://doi.org/10.1177/10946705241229419

Lee JK, Park J, Gregor S, Yoon V (2021) Axiomatic theories and improving the relevance of information systems research. Inf Syst Res 32(1):147–171. https://doi.org/10.1287/isre.2020.0958

Lemnitzer JM (2022) The implementation of the NIS 2 Directive: challenges and solutions. https://www.cbs.dk/files/cbs.dk/nis_2_implementation_supply_chains_report_7_september_2022.pdf. Accessed 22 Sep 2024

Ligthart A, Catal C, Tekinerdogan B (2021) Systematic reviews in sentiment analysis: a tertiary study. Artif Intell Rev 54:4997–5053. https://doi.org/10.1007/s10462-021-09973-3

Loebbecke C, Picot A, de Marco M, Newell S, Majchrzak A (2012) Information systems academicians supporting political decision making: towards expanding impact and relevance? In: ECIS Proceedings, Barcelona

Loomis JM, Blascovich JJ, Beall AC (1999) Immersive virtual environment technology as a basic research tool in psychology. Behav Res Meth Instrum Comput 31(4):557–564. https://doi.org/10.3758/BF03200735

Meißner M, Pfeiffer J, Pfeiffer T, Oppewal H (2019) Combining virtual reality and mobile eye tracking to provide a naturalistic experimental environment for shopper research. J Bus Res 100:445–458. https://doi.org/10.1016/j.jbusres.2017.09.028

Mohajeri K, Leidner D (2017) Towards a typology of relevance. In: HICSS Proceedings, Waikoloa Village, pp. 5783–5792

Monteiro J, Barata J (2024) The circular digital twin: climate-smart soils as a use case. In: ISD Proceedings. https://doi.org/10.62036/ISD.2024.107

Nandwani P, Verma R (2021) A review on sentiment analysis and emotion detection from text. Soc Netw Anal Mining 11:1–19. https://doi.org/10.1007/s13278-021-00776-6

Nunamaker JF Jr, Briggs RO, Derrick DC, Schwabe G (2015) The last research mile: achieving both rigor and relevance in information systems research. J Manag Inf Syst 32(3):10–47. https://doi.org/10.1080/07421222.2015.1094961

Orlikowski WJ, Iacono CS (2001) Research commentary: desperately seeking the "IT" in IT research – a call to theorizing the IT artifact. Inf Syst Res 12(2):121–134

Österle H, Becker J, Frank U, Hess T, Karagiannis D, Krcmar H, Loos P, Mertens P, Oberweis A, Sinz EJ (2011) Memorandum on design-oriented information systems research. Eur J Inf Syst 20(1):7–10. https://doi.org/10.1057/ejis.2010.55

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–77. https://doi.org/10.2753/MIS0742-1222240302

Peukert C, Weinhardt C, Hinz O, van der Aalst WM (2022) Metaverse: how to approach its challenges from a BISE perspective. Bus Inf Syst Eng 64(4):401–406. https://doi.org/10.1007/s12599-022-00765-9

Pfeiffer J, Duzevik D, Rothlauf F, Bonabeau E, Yamamoto K (2015) An optimized design of choice experiments: a new approach for studying decision behavior in choice task experiments. J Behav Decis Mak 28(3):262–280. https://doi.org/10.1002/bdm.1847

Pfeiffer J, Pfeiffer T, Meißner M, Weiß E (2020) Eye-tracking-based classification of information search behavior using machine learning: evidence from experiments in physical shops and virtual reality shopping environments. Inf Syst Res 31(3):675–691. https://doi.org/10.1287/isre.2019.0907

Pfeiffer J, Gutschow J, Haas C, Möslein F, Maspfuhl O, Borgers F, Alpsancar S (2023) Algorithmic fairness in AI: an interdisciplinary view. Bus Inf Syst Eng 65(2):209–222. https://doi.org/10.1007/s12599-023-00787-x

Plachkinova M, Faddoul G (2022) Using design science research to develop a secure social platform for complementary and alternative medicine. In: HICSS Proceedings, pp. 4157–4165. http://hdl.handle.net/10125/79843

Richter F, Koch P, Franke O, Kraus J, Kuruc F, Thiem A, Högerl J, Heine S, Schöps K (2020) Open discourse, V4 edn. Harvard Dataverse. https://doi.org/10.7910/DVN/FIKIBO

Romm C, Rice R, Cecez-Kecmanovic D, Jordan E, Pliskin N, Sudweeks F, Bjoern-Andersen N (1997) Panel 9 playing politics with information technology: a global perspective. In: ICIS Proceedings, Atlanta, pp. 522–524

Rupp C (2024) Navigating the EU cybersecurity policy ecosystem – A comprehensive overview of legislation, policies and actors. interface Tech analysis and policy ideas for Europe e.V. https://www.interface-eu.org/publications/navigating-the-eu-cybersecurity-policy-ecosystem. Accessed 27 Sep 2024

Saunders M, Lewis P, Thornhill A (2016) Research methods for business students, 8th edn. Pearson

Shanbhag N, Dawson M, Etori N (2024) Artificial intelligence's role in cybersecurity and global dynamics. In: MWAIS Proceedings, Peoria

Shekhar S, Petropoulos G, van Alstyne MW, Parker G (2022) Mandated platform compatibility: competition and welfare effects. In: ICIS Proceedings, Copenhagen

Sinha U, Muktevi LP (2024) Artificial intelligence in cybersecurity: a new paradigm revolutionizing threat intelligence and defense mechanism. In: AMCIS Proceedings, Salt Lake City

Spiekermann S, Krasnova H, Hinz O, Baumann A, Benlian A, Gimpel H, Heimbach I, Köster A, Maedche A, Niehaves B (2022) Values and ethics in information systems: a state-of-the-art analysis and avenues for future research. Bus Inf Syst Eng 64(2):247–264. https://doi.org/10.1007/s12599-021-00734-8

Straub DW, Ang S (2011) Rigor and relevance in IS research: redefining the debate and a call for future research. MIS Q 35(1):iii–xi. https://doi.org/10.2307/23043485

European Union (2024) Digital Europe programme (2021–2027). https://eur-lex.europa.eu/EN/legal-content/summary/digital-europe-programme-2021-2027.html. Accessed 17 Sep 2024

Vainionpää F, Väyrynen K, Lanamaki A, Bhandari A (2023) A review of challenges and critiques of the European Artificial Intelligence Act (AIA). In: ICIS Proceedings, Hyderabad

van der Aalst W, Bichler M, Heinzl A (2016) Open research in business and information systems engineering. Behav Res Meth Instrum Comput 58(6):375–379. https://doi.org/10.1007/s12599-016-0454-0

van der Aalst W, Hinz O, Weinhardt C (2020) Impact of COVID-19 on BISE research and education. Bus Inf Syst Eng 62(6):463–466. https://doi.org/10.1007/s12599-020-00666-9

Venkatesh V, Morris MG, Davis GB, Davis FD (2003) User acceptance of information technology: toward a unified view. MISQ 27(3):425–478. https://doi.org/10.2307/30036540

Weber P, Werling M, Baars H (2023) Design principles for institutionalized data ecosystems–results from a series of case studies. In: Wirtschaftsinformatik Proceedings, Paderborn

Weigl L, Barbereau TJ, Sedlmeir J, Zavolokina L (2023) Mediating the tension between data sharing and privacy: The case of DMA and GDPR. In: ECIS Proceedings, Kristiansand

Weinhardt C, Fegert J, Hinz O, van der Aalst WM (2024) Digital democracy: a wake-up call – how IS research can contribute to strengthening the resilience of modern democracies. Bus Inf Syst Eng 66(2):127–134. https://doi.org/10.1007/s12599-024-00862-x

Werling M, Lachenmaier J, Renken S, Lasi H (2022) Vertrauenswürdiger Datenaustausch in Ökosystemen – Entwicklung eines Metamodells zur Trennung von Daten und Kontext. In: Wirtschaftsinformatik Proceedings, Nürnberg. https://aisel.aisnet.org/wi2022/design_science/design_science/2

Wu SP-J, Straub DW, Liang T-P (2015) How information technology governance mechanisms and strategic alignment influence organizational performance. MISQ 39(2):497–518. https://doi.org/10.25300/MISQ/2015/39.2.10