Chapter 2
Digital sovereignty: a new perspective focused on data control

JEANNE C.M. VALLETTE D'OSIA, ELENA RAGAZZI, UGO FINARDI

CNR-IRCrES, Consiglio Nazionale delle Ricerche – Istituto di Ricerca sulla Crescita Economica Sostenibile, Strada delle Cacce 73, 10135 Torino, Italia

Corresponding author: jeannecharlottemarievallettedosia@cnr.it

ABSTRACT
Assessing data preferences is challenging, since digital privacy is often perceived as a fundamental societal need or right, rather than a good with an assignable market value. "Digital sovereignty: a new perspective focused on data control" is the second chapter of the Quaderno IRCrES *Cybersecurity and data protection in the electricity sector: state-of-the-art of the literature and evaluation methods* presents a literature review of studies that aim to evaluate individuals' digital privacy preferences in order to address the topic of digital sovereignty, which is closely linked to cybersecurity as it encompasses the procedures that make the digital environment more secure. Specifically, this section of the volume seeks to clarify the key concepts and definitions underlying digital sovereignty, while also reviewing the current state of research on the evaluation of personal data. We examine the challenges, such as behavioural and cognitive biases, as well as context-specific factors, that hinder the users' ability to assess their privacy and risk preferences, leading to a discussion of what the literature has identified as the Privacy Paradox.

KEYWORDS: Digital sovereignty, data privacy, data preferences, privacy paradox, behavioural biases.

DOI: 10.23760/2499-6661.2025.24_02
ISBN: 978-88-98193-39-4
ISSN (online): 2499-6661

HOW TO CITE
Vallette d'Osia, J.C.M., Ragazzi, E., & Finardi, U. (2025). Digital sovereignty: a new perspective focused on data control. In Ragazzi, E., Finardi, U., & Vallette d'Osia, J.C.M. (eds.). *Cybersecurity and data protection. in the electricity sector. State-of-the-art of the literature and evaluation methods* (pp. 27-43). Quaderni IRCrES 24. CNR-IRCrES. http://dx.doi.org/10.23760/2499-6661.2025.24_02

1 KEY CONCEPTS AND BEHAVIOURAL ECONOMICS: HOW IS DIGITAL SOVEREIGNTY PERCEIVED?

The aim of this literature review is to provide an overview of the theoretical and empirical literature on the economics of digital sovereignty, trying to answer the following question: how is digital sovereignty perceived at the individual level, and how can its value be assessed? This first section aims to describe, from an economic perspective, the key concepts and definitions underlying the research theme of digital sovereignty; in order to, in a second stage, support the review of studies that intend to measure it.

1.1 What is digital sovereignty and why is it important for economists?

The European Parliamentary Research Service (EPRS) defines digital sovereignty at the European level as: "Europe's ability to act independently in the digital word and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)" (Madiega, 2020, p.1). In this way, digital sovereignty includes the notions of data storage, data process and data governance, entailing a regulatory power on the use of data and the access to digital infrastructure. In his book entitled "Sovranità Digitale"[1] (2025), the founder and first director of Italy's National Cybersecurity Agency (ACN), Roberto Baldoni, gives a definition of digital sovereignty at the country level, based on four principles:

- full authority over the data generated by a nation's citizens, government and businesses,
- ability to employ secure technologies and expert workforce,
- existence of international collaborations to proactively address threats, and finally
- awareness and education about risks in cyberspace at the society's level.

With those principles, Baldoni (2025) explains that this definition of digital sovereignty describes a static and ideal situation, while in reality digital sovereignty is a dynamic concept, by being at the intersection of digital, geopolitical and economic transformations. With the gap between a country's actual level of digital sovereignty and the ideal outlined by these principles being its systemic vulnerability to cyberthreats.

In the 2000s, The European Union (EU) faced a major challenge regarding the protection of personal data[2]: the internal market was highly fragmented due to the lack of uniformity among the Member States' legislation on data protection (European Commission, 2010). In order to tackle cross-border data protection matters and revise the existing legal framework, namely the 1995 Data Protection Directive[3] which aimed to harmonize data protection rules at the EU level, the European Parliament and the Council approved the Regulation (EU) 2016/679 in April 2016, creating the well-known General Data Protection Regulation (GDPR)[4].

The GDPR standardizes data protection rules across the EU with guidelines for the collection and processing of personal data. More precisely, it allowed for the establishment of new rights and strengthening of already existing ones in the digital environment, offering more effective

[1] Translated in "Digital Sovereignty"

[2] "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". G.D.P. Regulation 2016/679, p. 33, Art. 4 (1).

[3] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[4] G.D.P. Regulation (GDPR) (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). (2016). (OJ L 119, p. 1-88).

control of individuals over their own data. One example of an existing right that required clarification is the *right to be forgotten*: the right of individuals to obtain from a data controller the erasure of their personal data without undue delay. Under the GDPR, this right was expanded and explicitly adapted to address the challenges of digital environments. In contrast, the *right to data portability* represents a newly established right: it allows individuals to receive their personal data from an organisation in a commonly used form, enabling them to easily transfer it to another service provider.

This global regulation on data privacy was therefore a requirement to allow people to share their data trustfully and in turn, to make the market for personal data efficient.

Our objective is to explore how the concept of digital sovereignty can be meaningfully applied at a narrower level: the individual one. We aim to understand how individuals' agency over the control of their data can be evaluated. Making an analogy with the above-mentioned principles relating to the concept of digital sovereignty at a nation's level, digital sovereignty for citizens would be a citizen's authority over the data they generate, which includes their ability to employ secure technologies to process their data, supported by a reliable data environment. It also involves their awareness and education about the risks present in the cyber-environment.

Therefore, digital sovereignty for individuals would be citizens' right and ability to have control over their personal data, grounded in the economic notion that data, like any other goods, belongs to the individual, who thus holds the right to use it and benefit from its value.

While they are linked to each other, the notions of digital privacy and digital sovereignty are different, as the former refers to the right to prevent any other entity from accessing personal data without the individual's consent. Digital privacy entails the existence of data protection instruments, from technical instruments such as an antivirus software to legal and regulatory instruments such as the GDPR. In turn, these regulatory instruments enable a data market to exist, giving space for the concept of digital sovereignty to be adapted at the citizen's level. Figure 1 summarizes the links between the two concepts of data privacy and digital sovereignty according to our vision.

To our knowledge, no other study in the current literature has drawn such parallel between digital sovereignty and the individual level. Works attempting to give an economic value to personal data have only focused on measuring digital privacy or data privacy, with those terms used interchangeably. Goldfarb & Que (2023) studied the topic from an economic perspective. They defined digital privacy as a term that "denote(s) a restriction on digital data flows" (p. 268), encompassing the dimensions of costs and benefits of restricting data sharing. More precisely, the authors explained how digital privacy has both an intrinsic and an instrumental value, which in other words means that digital privacy can be seen respectively as a final and an intermediate good. Indeed, sharing data is in itself an action that brings different levels of utility to people (what is considered "disclosable information" differs across individuals) and data holders, but it can also be seen as a mean to protect or hamper other's autonomy. It can do so directly, for instance in cases of sharing a list of contacts, or also indirectly, through a data-generating process (choosing to withhold data already gives market information) or probabilistic information (information about one person can reveal information about others). Thus, data flows present features of public good as they appear to be nonrival (the consumption of the good by one individual does not reduce its availability for others) and difficult to exclude (it is complicated or impossible to prevent others from accessing or using the good): in fact, shared personal information can often be duplicated and accessed by others. These first specific features characterizing digital privacy raise questions about how to adequately assess digital sovereignty from an economic viewpoint. In the following parts of this chapter, the analysis of digital sovereignty at the citizens' level will include a review of the literature that intends to quantify 'personal digital privacy' (or 'personal data privacy') as both notions are used when examining the data market from the individuals' perspective.

In their work on Economics of Privacy, Acquisti, Taylor & Wagman (2016) detailed more precisely the characteristics of privacy under the economic lens. Primarily, digital privacy generates information asymmetry, within an intertemporal scheme. In a first stage, before any disclosing of their personal data, individuals hold more information than service providers, such

as their consumption preferences, creating a first imbalance in the market. In a second stage, upon disclosing personal information, some immediate benefits appear for data subjects, such as for instance gaining a discount in exchange of sharing information. At a third stage, once data holders acquire individuals' information, they might be able to use it in ways not anticipated by data subjects, creating ambiguous and potentially long-term costs for the individuals. This can lead to price discrimination: through the analysis of consumers' purchase or location history, or also browsing behaviours, sharing personal information can become a tool for companies to segment customers, by extracting consumer surplus (the difference between what consumers would be willing to pay for a good and the actual price they pay), and targeting them with different prices.

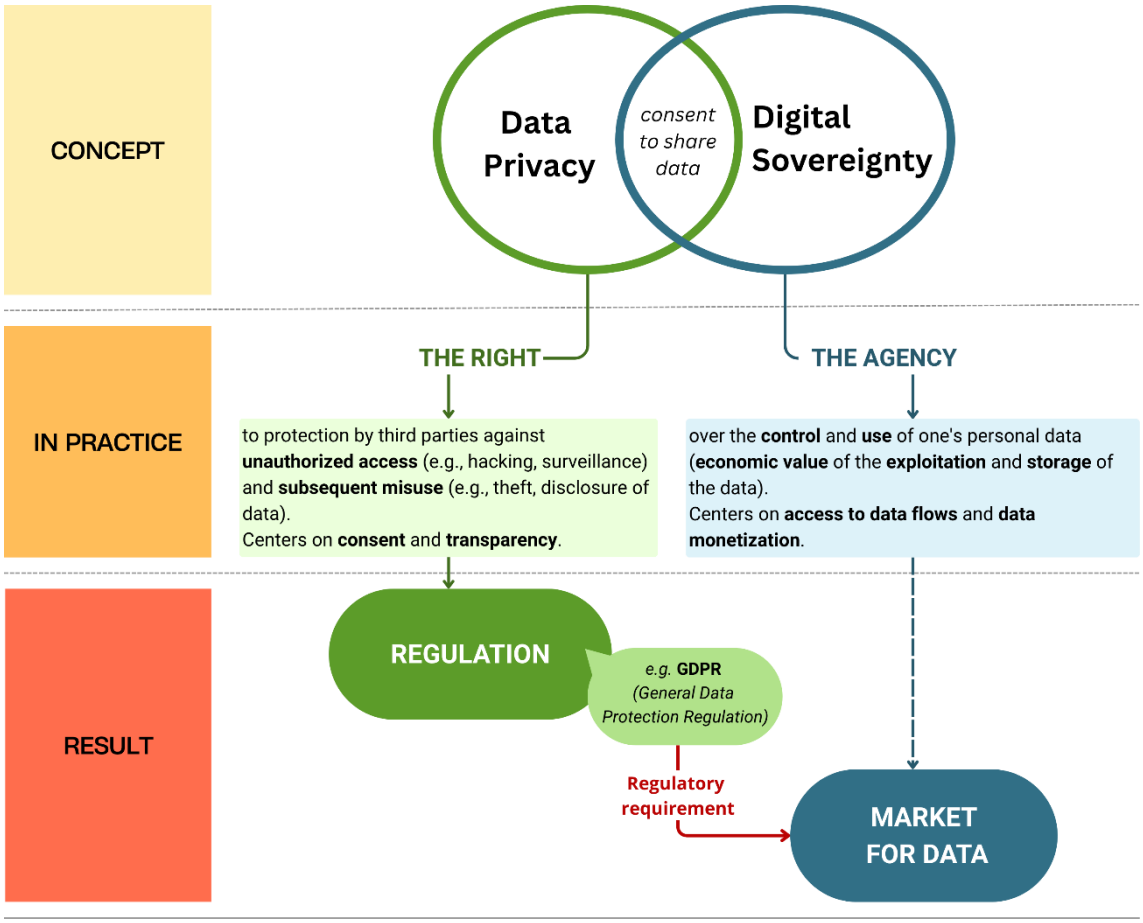
We mentioned the ideas of information asymmetry and intertemporality in disclosing personal data, but another feature described by Acquisti et al. (2016) is the tangibility of privacy trade-offs. The example of getting a discount after disclosing personal information is indeed tangible, but the emotions associated with sharing personal data, or potentially having them exposed, are intangible and add complexity to assessing the value of sharing data.

Furthermore, the authors pointed out a dual dimension behind the multiple definitions of data privacy in the literature: there is the notion of privacy as "control over usage" but also as "protection against access" (Acquisti et al., 2016, p. 449). This has important consequences for valuation, policy implication and regulation design. While control over personal information can protect individuals from the economic leverage that firms may gain by acquiring their data, it can also allow individuals to strategically withhold information to negotiate better prices or discounts. In our attempt to define digital sovereignty for individuals, we thus see this duality behind the notion of data privacy as the difference between data privacy and digital sovereignty, with the *control over usage* of personal data being the concept behind digital sovereignty and *protection against access* being the data protection right, stemming from the notion of data privacy. In this chapter, digital privacy is defined in terms of the disclosure of personal data, therefore studies that explore the consequences of such disclosure are examined. Finally, having defined the characteristics of privacy, Acquisti et al. (2016) demonstrated how trade-offs associated with digital privacy have direct and indirect costs and benefits. As mentioned above, by sharing personal information, data subjects can directly obtain discounts or personalized services. Another kind of benefit lies in the saved opportunity cost: by divulging personal data, people can reduce their search costs and receive more accurate information. Reading the situation from an economic perspective, these benefits become opportunity costs in the case of someone choosing not to disclose its data. This cost-benefit approach enables us to perceive how it may be possible to value digital sovereignty.

To fully analyse digital sovereignty, another important aspect, that of cybersecurity, needs to be considered. Cybersecurity is a tool used to reach digital sovereignty: it enables control over data through the protection against cyber breaches of systems and networks at global level and, in turn, of personal data at narrower levels. Kianpour, Kowalski & Øverby (2021) explained that "cybersecurity deals with the different procedures that create a secure environment by protecting the assets" (p. 3).

In this first descriptive section, we have exposed the complexity behind the economic lecture of digital sovereignty and defined the main concepts bounded to it. In our view, digital sovereignty for individuals refers to the *right and ability of citizens to control and benefit from the use of their personal data*, supported by secure technologies and a trustworthy data environment. It is grounded in the idea that personal data, like any economic good, belongs to the individual. In contrast, digital privacy concerns the *right to prevent unauthorized access* to personal data. While related, the two concepts differ with privacy protecting access and sovereignty empowering usage. Legal and technical data protection instruments such as the GDPR make this distinction effective in practice by enabling individuals to exercise both protection and control.

Figure 1. Conceptual framework of the concepts of Data Privacy and Digital Sovereignty



1.2 Context dependency, cognitive biases and heuristics in privacy decision-making

Building on the definition and characteristics of digital sovereignty, this section explores how individuals' decisions regarding digital privacy are shaped by behavioural biases and contextual factors. While sharing personal data involves complicated trade-offs due to the complex nature of privacy as a good, people's valuation of these trade-offs is often influenced by cognitive biases and specific settings. Understanding these biases, along with the contextual specificity of privacy choices, provides deeper insight into how individuals miscalculate risks related to data privacy and, consequently, possibly incorrectly estimate how much they care about the sharing of their personal data.

An important aspect repeatedly underlined by the literature on the value of digital privacy, is that it is highly context dependent. In a report already published in 2013 entitled "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", the OECD highlighted the sensitivity of privacy and data valuation to contextual factors, emphasizing that estimations of the monetary value of personal data can differ across scenarios.

To illustrate context-dependency, one can take the common example of individuals who might be willing to share location data for navigation purposes, but would likely withstand disclosing the same information for targeted advertising – not necessarily due to the advertising itself, but due to the discomfort or even anxiety coming from a lack of transparency in how personal data are used to deliver personalized content. This example might be trivial as there are rational reasons explaining it, while other cases might appear more problematic because they are driven by less rational behaviours, such as individuals who may refuse to share the location of their mobile device with their relatives, even though doing so would facilitate finding it when misplaced for instance, while simultaneously consenting to location tracking by online platforms. Behind this

example lies the idea that individuals might fear sharing personal information to people that they know while unknown-online persons might appear to be less threatening.

These examples illustrate how the perceived value of privacy trade-offs is shaped by the purpose of data collection, the identity of the data collector, and the expected use of the data, making privacy valuation variable across different settings.

Bansal, Zahedi & Gefen (2016) empirically tackled the question of context dependency in privacy with a multidisciplinary study. Through an experiment using contextualization of Theory of Reasoned Action ("TRA-privacy") and Prospect Theory, they tested, among others, three hypotheses regarding trust, privacy concern and context sensitivity on disclosing private information. The use of TRA-privacy enabled to study context-related antecedents (personality and experience) of survey-takers and context-specific disclosure of private information, while Prospect Theory provided insights on the utility (or disutility) of individuals to disclose private information, and whether it varies across contexts. More precisely, they compared three contexts in their experiment, using finance, ecommerce and health websites to respectively encompass high monetary context sensitivity, low monetary context sensitivity and sensitive social-based context sensitivity. Their results showed that trust was positively associated with intention to disclose information, with a more significant role in a sensitive social-based context (health) compared to monetary ones (finance and ecommerce). On the contrary, they demonstrated that the relationship between privacy concern and intention to disclose information was significantly negative. Finally, their experiment revealed that privacy concern influenced trust only in sensitive monetary contexts, as the negative relationship between privacy concern and trust was indeed significant in the finance context but not in the ecommerce and health ones. Overall, these findings support the links between trust, privacy concerns and context sensitivity, reinforcing the argument that digital privacy behaviours are highly context-dependent, and therefore difficult to appraise. For what concerns experience, the authors found that previous experience with privacy invasion had an impact on both intentions to disclose and privacy concern. More precisely, they assessed that privacy concern, regardless of context, increased with prior negative experiences of privacy breach. Subsequently, they showed that prior positive experience with a website, especially in ecommerce contexts, had a positive association with intention to disclose data.

Chen, Gu, Wei & Lv (2023) studied the relation between privacy invasion experiences and protection intentions in social media contexts. They validated the hypothesis that prior privacy invasion experiences positively impacted privacy protection intentions. However, they advanced that this relationship was mediated by response costs (any costs such as monetary, time and effort of resulting protective actions) and the phenomenon of privacy fatigue, which they defined as "the complexity of the measures required to protect personal information aggravates user's sense of futility, leading to exhaustion among online users." (p. 2).

In an earlier work, Acquisti, Brandimarte & Loewenstein (2015) published a review entitled "Privacy and human behaviour in the age of information" in which they dug into key themes regarding privacy-related behaviours. Two of these themes are especially relevant for the understanding of context specificity. First, they specified that privacy norms are dictated by culture, time, situation and motivation. To justify this statement, the authors cited studies that looked at individuals' behaviours in diverse contexts, for instance where personal information was either revealed to friends or to strangers (Stutzman, Gross & Acquisti, 2013) or, where individuals were confronted with diverse websites interfaces (John, Acquisti & Loewenstein, 2011), or lastly where individuals were given information about others' behaviours regarding the same survey they had to take (Acquisti, John & Loewenstein, 2012). Results always showed that the group or situation individuals were assigned to was driving their disclosure of information in significative ways, thus underlining the context-dependence of privacy concern. Secondly, Acquisti et al. (2015) raised the topic of uncertainty, regarding both individuals' own privacy preferences and their awareness of what information they are sharing, with whom, and how it might be used. The authors argued that not only when there was information asymmetry, but also when people were aware of the consequences of privacy decisions, individuals were unclear about their privacy concerns and preferences. They detailed that not only social norms, emotions, heuristics, but also the desire for interaction, disclosure and recognition were motives behind

privacy preference uncertainty. By leading people to be undecisive, uncertainty can amplify context-dependence: individuals not being able to clearly identify their privacy preferences would try to detect signals in their environment that would provide them with guidance for privacy choices, making context-dependency even more prevalent.

We now delve into these cognitive, psychological and behavioural biases that distort in multiple ways individuals' uncertainty regarding sharing sensitive information, since other factors than purely contextual ones might worsen the assessment of digital privacy. Indeed, context dependency was mentioned by the authors cited in the previous section, but Goldfarb & Que (2023) also pointed out that not only privacy concerns are dependent on context, but they increase over time, "driven by an expansion of the types of data that consumers consider to be private" (p.270) while Acquisti et al. (2016) underlined that privacy concerns are also inherently diverse, as they take roots in individuals' traits and attributes.

One self-explanatory bias lies in the complexity and overload of data privacy information, also described as bounded rationality (van Ooijen & Vrabec, 2019; Acquisti et al., 2015). In fact, one can easily picture how fragmented and dense is the information about privacy policies, and terms and conditions of the number of websites we visit, mobile applications we download and online services we use in our daily life. To illustrate this, van Ooijen & Vrabec (2019) mentioned a Norwegian campaign-group who exposed that only reading terms and conditions of 33 typical smartphone apps would take nearly 32 hours (Palazzo, 2016). Evaluating what consenting to those terms actually entails would take even more time, creating an additional burden. The same authors, along with Acquisti et al. (2015), quoted another study to illustrate this phenomenon: after analysing 64 online privacy policies of US companies, Jensen & Potts (2004) found that almost half of them were not sufficiently accessible for most Internet users.

Bearing this in mind, another cognitive bias intervenes when accepting terms and conditions or privacy settings. It has been shown in the literature that default settings of websites, apps and other internet services are often interpreted by individuals as implicit recommendations, leading them to accept privacy settings more advantageous for the firm than for themselves (van Ooijen & Vrabec, 2019; Acquisti et al., 2015; Acquisti, Brandimarte & Loewenstein, 2020).

Moreover, Kianpour et al. (2021) mentioned three biases leading to incorrect beliefs about data privacy, namely the "law of small numbers", the "projection bias" and "overconfidence" or "illusory control" (on the topic see Acquisti et al., 2020). The law of small numbers skews perception by making individuals draw broad conclusions from limited experiences, for example, overestimating/underestimating privacy risks due to a lack of personal (or from peers) negative incidents, or overestimating/underestimating the efficacy of certain cybersecurity practices based on anecdotal success stories. Similarly, overconfidence can lead individuals to overestimate their capacity to detect or respond to cyber threats, creating a false sense of control and encouraging riskier behaviour when disclosing personal data. Finally, projection bias causes individuals to assume that their current attitudes and behaviours toward privacy will remain stable over time and are shared by others. Such assumptions can lead to the oversharing of personal data – or to the non-adoption of necessary protections – and to the expectations that others will act similarly, creating a feeling of trust that could be misplaced.

In a more extensive study about consumer privacy decision-making, Acquisti et al. (2020) described additional psychological factors affecting individuals' choices. Among them, the "present bias", the "adaptation bias" and the "drive to share" complexify the ability to align behaviour with long-term privacy interests. Indeed, the present bias leads individuals to prioritize immediate rewards over long-term consequences. As a result, people may willingly share personal data to receive small, short-term benefits, such as online discounts or quicker access to services, while underestimating the lasting and less visible costs, such as intrusive profiling or unexpected targeted advertising based on data profiling. Furthermore, even when the underlying risks of surveillance or data breaches persist or worsen, individuals may become less responsive, perceiving the problem as either unsolvable at their level or no longer urgent, creating an adaptation bias. Lastly, the drive to share reflects the powerful motivational forces behind self-disclosure, particularly in social media contexts. Individuals often disclose personal or even sensitive information online (such as location data) not because they undervalue privacy, but

because competing incentives driven by social connection are perceived as more immediate or emotionally rewarding.

This section detailed how human decision-making regarding personal data disclosure is shaped by psychological, behavioural and contextual factors. With very intertwined and sometimes reciprocal links - uncertainty about which personal data can be safely shared can lead to inaccurate assessments of cyber risks, while, conversely, a lack of clear understanding of those risks can create ambiguity in individuals' digital privacy preferences -, these factors impede the correct appraisal of individuals' data privacy. These factors are therefore the core reason behind what the literature defines as the "privacy paradox", the discrepancy between individuals' stated privacy expectations and data market behaviours, which we will investigate in the following sections. Indeed, we will now review some empirical studies that intend to evaluate data privacy at the individual level, to then examine the privacy paradox that some of them reveal.

2 Economic valuation of Digital Sovereignty: measures of costs and incentives of sharing personal data

This section tackles studies that seek to quantify individuals' perceptions of risk and preferences regarding their personal data. The review will show that valuing (or monetizing) individuals' digital privacy, often operationalized through the act of data sharing, relies mostly on empirical approaches which fall under the umbrella of stated-preference methods in recent literature. Besides, the economic assessment of digital privacy brings up a discrepancy between the desired and realized online privacy decisions, known in the literature as the privacy paradox. We address the discussion surrounding this concept in the last subsection of this chapter.

2.1 Valuation techniques and estimations of data privacy

The definition of privacy valuation we align with in this review is the one stated by Goad, Collins & Gal (2021), which involves the idea of privacy -preference, -concern and -calculus: "Privacy Valuation is the monetary value, which an individual assigns to a Privacy Preference and is essentially one form of quantification of that preference." (p.4), with "Privacy Preference [being] the choice between alternatives as they relate to decisions about controlling information about oneself." (p. 4). As digital sovereignty entails that individuals benefit from the value of their personal data, the idea that there should be a consecutive reward to the consent of sharing personal data must be kept in mind in addition to that of simple protection entailed by digital privacy.

To ensure the relevance and manageability of the reviewed literature, the search was limited to studies employing individuals' valuation methods applied to online privacy, from 2020 onwards. This choice of timeframe has both practical and substantive reasons. Indeed, the literature on the topic appeared in the late 1990's (see for instance Ackerman, Cranor and Reagle, 1999) and grew rapidly along with the importance of online services, leading to a substantial number of publications, impractical to include given spatial and temporal constraints. Moreover, as discussed in the previous section, the valuation of data privacy is highly context-dependent and sensitive to evolving digital environments, norms, and regulatory frameworks. Focusing on recent contributions allows for a more accurate reflection of current user attitudes and market conditions.

This analysis prioritizes individuals' valuation methods over market-based approaches (categories outlined by the OECD, 2013) because this study focuses on consumers' own perceptions of privacy value. Rather than examining the market value of data from a business-model perspective, the aim is to understand how individuals subjectively assess the value of their personal information. Moreover, market valuation methods often fail to account for externalities (Malgieri & Clusters, 2017), a dimension we explicitly aim to capture in this study.

Hence, the following studies all intend to disentangle individuals' awareness, concerns and preferences and in turn attempt to value the protection of privacy online. Among other features, they differ in the online themes and services they observe.

For instance, studies by Blythe, Johnson & Manning (2020) and Goad et al. (2021) were anchored in the concept of the Internet of Things (IoT), focusing on individuals' behaviours towards internet-connected devices, while Jung, Shin & Kim (2025) along with Yamaguchi, Oshima, Saso & Aoki (2020) explored the handling of personal information on social media.

The study by Blythe et al. (2020) focused on the UK and was based on a contingent valuation method (CVM) to measure the willingness to pay (WTP) for improved security in specific connected products (i.e. smart watch, smart thermostat, WI-FI router, smart TV and security camera). Unsurprisingly, the authors observed that consumers would pay more for more secure devices, even though this varies across the type of product under consideration (e.g. respondents cared more about their Wi-Fi Router and Security Camera being secure than their smart TV). More specifically, they found that presenting security-related information prior to asking about people's WTP did encourage consumers to pay more for secure devices, indicating that security information influences purchasing behaviours. However, they assessed whether the WTP was influenced by the relative improvement in security, which turned out to not be the case after testing for both a 50% and a 90% improvement in security afforded: enhancing security itself, regardless of its magnitude, affects individuals' purchasing behaviours.

Controlling for more attributes that affect privacy preferences, Goad et al. (2021), employed a discrete choice experiment (DCE) to their US sample to compute both individuals' WTP for beneficial features that improve privacy and willingness to accept (WTA) infringements on their privacy for a specific connected device: a fitness tracker. In exploring contexts, information type and personal characteristics through the choice tasks they submitted to participants, the authors found that some personal characteristics, namely age and gender, impact privacy preferences and argue for a "right amount of privacy" (p. 14) with a strong variation in WTA according to the type of private information. These findings underline how essential it is to assess the type of information, the context, the individual in question, but also the level of process, procedures and technology operated by organizations prior to deploying privacy solutions.

Though applied to online services in South Korea, the CVM study by Jung et al. (2025) supports similar arguments: sociodemographic features impact the monetary value of people's SNS (social networking services) privacy: "[…] highly educated young adults in their 20s or 30s, on average, put the highest monetary value on SNS privacy" (p. 1106), and SNS users who use platforms for personal purposes such as "friendship" and "self" tend to value their privacy more than those who use them mainly for information sharing. Overall, they estimated the monetary value of SNS privacy at $27.83 (how much participants are willing to accept to disclose their personal information on SNS by accepting a friend request from a marketing firm, which corresponds to how much compensation respondents would accept for the loss of SNS privacy in the paper).

Among other online services categories (such as messaging apps, online news, and search engines), Yamaguchi et al. (2020) also explored data utilization within social media. They used a CVM to uncover the amounts of WTP for data to be utilized or not utilized for the specific service in question, in Japan. Unlike Jung et al. (2025), the authors found that the WTP for social media services was positively associated with data utilization, as well as their internet literacy index. This finding suggests that greater familiarity with the Internet and social media allows individuals to better recognize the benefits of data use, such as the convenience of personalized services and targeted advertisements.

Other studies take a more service-specific approach, embedding privacy trade-offs within clearly defined usage contexts. For instance, Wein (2022) studied German users' preferences toward the artificial intelligence (language translator) DeepL in a controlled online experiment. The author employed control and treatment groups. The control group encompassed participants that could either use DeepL by accepting cookies (thus lowering their privacy) or opt out entirely and not use the service, while the two treatment groups reflected other privacy preferences, as, in addition, they could:

Group 1: choose a privacy-respecting version of DeepL by stating how much they were willing to pay for it (a self-reported WTP greater than zero).

Group 2: vote on whether they would pay a fixed, realistic fee (10€ annually) for a privacy-friendly campus version of DeepL. This group introduced a real market price to better reflect actual privacy preferences.

The author showed that introducing a monetary option for privacy significantly reduced participants' acceptance of cookies, thus giving up their data. In the control group, 79.31% accepted cookies, possibly due to cookie fatigue (dismissing cookie consent pop-ups without fully understanding the implications, potentially compromising privacy and data control), while 20.69% refused to use DeepL out of privacy concerns. In the treatment group with a self-reported WTP option, cookie acceptance dropped to 30.43%, and only 4.35% refused the service entirely. Finally, in the treatment group with a fixed fee for a privacy-friendly version, cookie acceptance further dropped to 27.91%, and just 2.33% refused DeepL altogether. Therefore, introducing a paid alternative for privacy reduced reliance on cookies and encouraged privacy-respecting choices, showing that people are more likely to protect their data when realistic options are available. Another insight was that 35% of the respondents in the self-reported WTP treatment group indicated a WTP less than 10€, suggesting that either their true WTP was indeed lower than 10€ or that they lacked a price reference, supporting the idea that market prices help clarify and reveal privacy preferences.

Similarly grounded in a specific online service, Paliński (2022) examined a ride-hailing service in Poland to estimate individuals' WTA personal data sharing in exchange for fare discounts. Using a DCE estimated with a mixed logit model, and a treatment and control groups as well, being respectively a group with the GDPR notice and one without, the author not only assessed users' readiness to share data for a discount on the final trip cost, but also investigated how awareness of digital rights under the GDPR influenced privacy preferences (for more empirical literature on the specific topic of GDPR's effects, see Goldfarb & Que, 2023 and Zamparini, 2024). The author found that reminding their GDPR rights to participants significantly increased the value they assigned to personal data protection, suggesting that legal awareness, rather than satisfying privacy concerns by giving a sense of control over privacy, seems to amplify them.

Another recent study aimed to measure individuals' WTA data sharing in exchange for a discount, this time using CVM through a five-point Likert-type willingness scale. D'Annunzio and Menichelli (2022) investigated both the willingness to share data for a discount (WSD), with the question "Which of the following types of personal data would you be willing to share to receive a price discount?" (p.578) and the WTP to protect data (WPP), with the question "For which of the following types of personal data would you be willing to pay a monetary price to keep private?" (p.578) in digital markets in Norway. This investigation illustrates how privacy preferences are not uniform but depend on how individuals weigh financial incentives against data sensitivity. Indeed, the study found that WSD (scale-reversed to be compared to WPP) was consistently higher than WPP across all types of personal data. However, the size of the gap between WSD and WPP was larger for highly sensitive data (e.g., credit card numbers, phone call and SMS content, pictures), in comparison with general, less sensitive, data (e.g., age, gender, name), indicating a stronger reluctance to share sensitive data, even for a discount.

Following the same goal to identify differences privacy preferences between data types, Skatova, McDonald, Ma & Maple (2023) examined whether participants in the UK were willing to pay to avoid sharing various types of data across different data sharing environments. They did so through five different evaluation techniques: two different WTP conditions and 3 additional conditions to elicit individuals' preferences to protect different types of data. This method allowed them to uncover whether stated preferences for keeping personal data private are stable within individuals and whether they systematically vary between data sharing environments. The study found that individuals' privacy preferences were stable and coherent across the different elicitation techniques, confirming the existence of well-defined privacy attitudes. However, the authors elicited three tiers of data, with the most valuable one encompassing banking transactions and medical records, while their second (browsing history, mobile phone GPS and social media) and third (electricity use, loyalty cards and physical activity data) tiers remained distinctively below in their ranking scores, which also illustrates the relative importance of protecting different

types of personal data. Goad et al. (2021) elucidated the same finding. In their case, personal health was also considered the most sensitive data type, along with physical location. These results emphasize a practical implication: there is no "one solution fits all" model for privacy concerns.

Cloos & Mohr (2022) also used a scenario-based approach to investigate how people value privacy in different environments. They presented respondents in their experiment with monetary benefits, either personal (treatment group 1) or environmental (treatment group 2), in exchange for data sharing. The environments in which the scenarios were taking place were the following: supermarket, in which data sharing could provide benefits on a loyalty card app; a health insurance company with potential benefits on a tracking bracelet app; the federal ministry of health with a nutrition app; a technology start-up company through a mobility tracking app; and finally, the energy provider with a smart meter app. The results indicated no treatment effects between the groups, but higher acceptance values for data sharing in the applications relatively more familiar to respondents, and among people with stronger green consumption values, higher risk propensity, or younger age show a higher acceptance of data sharing. Therefore, the study shows that acceptance depends more on the recipient of the data and the type of information shared than on the nature of the benefit.

Finally, another interesting characteristic was tackled by Prince & Wallsten (2022), namely a cross-country comparison, revealing significant cultural and contextual differences. Using discrete choice surveys conducted in the United States, Germany, and several Latin American countries (Mexico, Brazil, Colombia, Argentina), the authors estimated the WTA data sharing across various types of personal information (financial, biometric, location, browsing, etc.). They found that Germans valued privacy more than respondents in the U.S. and Latin America, with financial and biometric data being the most highly valued. International differences were even stronger regarding ads: in some Latin American countries, individuals were even willing to pay to receive targeted ads. This cross-national perspective shows that privacy policies should be tailored to national and cultural specificities.

All these empirical studies differed among them in their objectives and implementations, as some used treatment and control groups to test diverse framing effects or incentives, while others embedded privacy trade-offs in varied application environments (e.g., health, mobility, finance). After reviewing them one can validate the theoretical argument we exposed in the first section: *context and individual characteristics have significant roles in shaping privacy preferences and valuations*. Evidence that privacy calculus and valuation are influenced by the type of data, the recipient, and the context of data use was recurrently demonstrated. Moreover, these studies confirm that privacy preferences are neither fixed nor uniform across individuals or situations, rather, they reflect trade-offs between perceived costs and benefits.

Even though all the studies are based on similar measures in order to elucidate individuals' privacy preferences, mainly WTP for privacy or WTA data disclosure, it is important to note that a debate on their validity exists in literature. Winegar & Sustein (2019) intended to elucidate the disparities between WTP to maintain privacy and WTA to allow access to personal data, and they argued that "because of a lack of information and behavioural biases, both […] measures are unlikely to be reliable guides to the welfare effects of retaining or giving up data privacy." (p. 18). However, one limitation of their study is that it relied on directly asking participants to assign monetary value to their privacy, which is a task that can be difficult without prior experience. Eliciting economic value through responses to specific scenarios (thanks to DCE for instance) may yield more reliable results.

In addition, another theoretical aspect is worth underlining here. As explained by Prince & Wallsten (2020), measures of benefits of privacy protections cannot be interpreted as the net value of privacy. They take a practical example to illustrate this idea: they estimated consumers' value for keeping location data on a smartphone at $1.20, with the assumption that keeping location data private lowers accurate driving directions and concluded that "the net benefits of requiring smartphones to keep location data private would, therefore, be $1.20 minus however much people value high-quality directions on their phones." (p. 32).

Finally, one last theme repeatedly emerged in the above literature: the apparent gap between individuals' stated privacy concerns and their actual behaviour (Yamaguchi et al., 2020; Blythe et al., 2020; Goad et al., 2021). This discrepancy, known as the privacy paradox, will be the focus of the next section.

2.2 The discussion around the Privacy Paradox

The review of the literature on data privacy and its economic valuation reveals the ongoing debate about the so-called privacy paradox. Some authors argue for an irrational inconsistency in the privacy behaviours in comparison with people's stated preference (Yamaguchi et al., 2020), which concretely translates in "individuals [who] would indicate a higher preference for privacy than they would reveal in their everyday actions." (p. 4-5, Goad et al., 2021). Others argue that this discrepancy is better explained by bounded rationality and context-dependent cost-benefit reasoning, framing it as a "trade-off" rather than as a paradox (Wottrich, Van Reijmersdal & Smit, 2018). Finally, some scholars reject the notion entirely, claiming that the paradox is a myth as privacy attitudes and behaviours are incomparable (Acquisti et al., 2015; Solove, 2021). We delve into this discussion and analyse the studies that have been tackling this debate.

Multiple works have aimed to review the literature in order to disentangle the different explanations behind the privacy paradox, all taking roots on the one carried by Kokolakis (2017) (Bart & de Jong, 2017; Gerber, 2018; and Zamparini, 2024). The strategy of the initial study by Kokolakis (2017) was to review literature that supports or challenges the existence of a dichotomy between attitudes and behaviours, thus screening the debate around the privacy paradox. The author identifies three major limitations that undermine the privacy paradox as a fully robust theoretical construct: (1) contextual variability across studies, (2) inconsistent conceptual definitions, and (3) methodological disparities in research design.

We already elucidated in the previous section that the valuation of digital privacy is highly dependent on the context it is embedded in, which often leads to inconsistencies in stated preferences and realized intentions in privacy online. Kokolakis (2017) presented the example of a study that took place in a classroom, which can be classified as a familiar environment that probably led respondents to underestimate the risks of sharing personal information. In addition, the author emphasized that studies often examine different categories of personal information (e.g., demographic data, online behaviour, sensitive beliefs), which may not be directly comparable. They similarly highlighted how privacy concerns vary across three types, organizational threats (e.g., data misuse by companies), social risks (e.g., stalking), and unauthorized access by employers or the public, and therefore influence attitudes and behaviours to differing degrees.

For what concerns the theoretical background regarding research on the privacy paradox, Kokolakis (2017) provided a comprehensive review by listing five research themes: a) privacy calculus theory; b) social theory; c) cognitive biases and heuristics in decision making; d) decision making under bounded rationality and information asymmetry; and e) quantum theory homomorphism. In doing so, the author demonstrated that findings must always be interpreted in light of the researcher's underlying assumptions, which are shaped by their disciplinary lens (i.e., social theory, behavioural economics, psychology…). For instance, studying the privacy paradox as a trade-off, as argued under the privacy calculus theory, might lead to different conclusions than if it was studied under the scope of cognitive biases and heuristics, as the latter refutes the assumption of the former that individuals make privacy decisions as rational agents (see Section 1.2).

In a similar way, Bart & de Jong (2017) carried out a systematic review on the topic as well, with a focus on mobile computing, and considered online user's decision making under different lenses: (a) rational risk-benefit-calculation, (b) biased risk-benefit calculation and (c) no or only negligible risk consideration. These categories explain issues of information privacy and, in turn, the privacy paradox as, again, either rationality or influenced behaviour biases are reflected in the

results. The authors argued for mobile applications with mixed approach and design solutions adapted to different cognitive styles.

Methodological choices also matter in testing the presence of a privacy paradox. Kokolakis (2017), after observing that the most common approaches are surveys and experiments, concluded that experimental approaches used to address the validity issues did not recreate realistic contexts (e.g., studies were usually based on online questionnaires or convenience samples that were less robust than studies with factual data collected from a representative samples).

Gerber, Gerber & Volkmaer (2018) also agreed on methodological considerations explaining the privacy paradox. Their literature review, which identified the significant factors that predict privacy aspects, also assessed the theoretical privacy paradox explanations. About the methodological challenges, they underlined a strong limitation to many studies as behaviour was often assessed as a dichotomous answer while attitudes were measured on metric scales. They also dedicated a section of their paper to the assessment of predictors for different privacy aspects. In the first place, they showed that attitude towards privacy was studied through different variables, such as privacy attitude, privacy concerns or perceived privacy risk while intention and willingness to disclose data were used to assess privacy intentions, and privacy related behaviours were elucidated through disclosure of information, the actual usage of data sharing applications, the management of privacy settings and the performance of privacy protection behaviour. The multiplicity of predictor variables reflects the challenges in interpretability when debating the privacy paradox. Secondly, they observed that 'the privacy calculus' was the best approach, with 'gained benefits from disclosing data' being the best predictor for privacy behaviour (both for disclosing intention as well as actual disclosure) and the best predictor for privacy attitudes being internal variables like trust towards the websites, privacy concerns or computer anxiety.

However, two other works (Skatova et al., 2023; Glasgow, Butler & Iyengar, 2021) took into consideration these methodological challenges, trying to justify a potential privacy paradox, without finding significant results.

As mentioned in the previous section, Skatova et al. (2023) employed five different elicitation techniques, including WTP and various ranking methods, to examine whether individuals' preferences for protecting data were consistent across contexts and methods. In their cases, findings showed that rankings of data sensitivity were consistent across elicitation methods for most participants, particularly for highly sensitive data like banking or medical records. These results challenged the notion of a privacy paradox by demonstrating that people do have stable and structured privacy preferences. In addition, they supported the use of stated preference evaluation techniques as an appropriate methodological approach for uncovering people's underlying privacy preferences.

Glasgow et al. (2021) investigated whether survey methodology could explain the privacy paradox by comparing between-subject and within-subject designs in a discrete choice experiment based on hypothetical ride-hailing services. Contrary to their expectation, the results showed no statistically significant difference in privacy valuations between the designs. Notably, the within-subjects approach, which explicitly presented location sharing as an attribute in each choice scenario, failed to produce the hypothesized response bias that could have revealed a privacy paradox. The comparable outcomes across both designs suggest that methodological biases in survey design did not fully explain the discrepancy between stated privacy preferences and actual behaviour.

Drawing on the studies of Kokolakis (2017) and Gerber (2018), Zamparini (2024) reviewed theoretical and empirical studies regarding digital privacy, highlighting that privacy as a concept is strongly contextual, evolving over time, and that measuring digital privacy is subject to strong methodological challenges. For instance, the discrepancy between WTP to protect data and WTA compensation to share them reveals that privacy valuations vary significantly depending on the type of data, individual characteristics, and cultural context. He agreed with Gerber et al. (2018) and Kokolakis (2017), by stating that "the digital privacy paradox may be the result of the specific methodology that is used to test this hypothesis" (p. 154). The paper also situated the privacy paradox within the main public regulations on data privacy, such as the GDPR and its economic

effects, which stresses the need to interpret privacy preferences as highly contextual and shaped by institutional and informational environments.

Building on these studies and reviewing the literature on the privacy paradox and its applicable theoretical approaches, we now turn to the privacy calculus framework, identified by Gerber et al. (2018) as the most comprehensive explanatory model. Skatova et al. (2023) and Wottrich et al. (2018) illustrated well this theoretical approach. Indeed, both suggested that inconsistencies in behaviour, such as respondents sharing data despite stating they had a high concern for privacy, reflected trade-offs rather than irrationality. Wottrich et al. (2018) investigated privacy decision-making in the context of mobile app downloads through two online experiments. They framed the discrepancy between stated privacy preferences and actual behaviours as an economic trade-off where individuals weigh the perceived benefits of app use, defined as 'app value' against privacy costs, based on the concepts of "app intrusiveness" and "concerns". Their findings demonstrated that the benefits of using a mobile app significantly increased the likelihood of users' willingness to share data, to a greater extent than app intrusiveness and privacy concerns decreased it, even among users with high privacy concerns.

This highlights the context-dependent nature of privacy choices and illustrates bounded rationality, which refers to users' limited capacity to fully understand and evaluate all relevant information, even when that information is available, potentially leading to suboptimal or inconsistent decisions (Gerber et al., 2018). This study provides evidence that immediate benefits often outweigh privacy concerns, emphasizing that users do not disregard privacy irrationally, but make situational trade-offs.

The fact that Wottrich et al. (2018) argued for bounded rationality and context-dependency, is another common point shared with Skatova et al. (2023). In fact, the latter observed stability and structure in well-defined privacy preferences among their respondents, which suggests that there is not such a thing as a paradox. The thesis of stability of privacy expectations is also supported by Martin (2021) who used factorial vignette surveys to assess the extent and comparative significance of violating consumer privacy norms. First, she investigated the privacy paradox by testing its strong assumption (i.e., individuals give up privacy expectations after disclosure) and weak assumption (i.e., privacy is traded for benefits like better services or discounts). Contrary to these assumptions, her findings revealed that consumers do maintain privacy expectations post-disclosure and weigh how their data is used more critically than often assumed. To test privacy as a core value, the author compared privacy violations (e.g., third-party data sharing) with security breaches (e.g., hacking) and found that consumers perceived both as equally damaging to trust. The study challenges the privacy paradox by showing that users view online tracking and secondary data use as serious trust violations, undermining the notion that they willingly sacrifice privacy for convenience.

Finally, some authors argue that the privacy paradox is a misconception. Since privacy preferences are defined broadly while behaviours are analysed in very specific contexts, conclusions about people's valuation of privacy are impossible to compare to their privacy decisions. Acquisti et al. (2015) argued that privacy attitudes and behaviours should not be expected to be closely related, which Solove (2021) supported by concluding its article entitled "The Myth of the Privacy Paradox" that "[…] the gap between privacy behaviour and attitudes is not an anomaly that should be rectified; the gap exists because the behaviour and attitudes are about different things. The effort to try to align them falters because they cannot be fully aligned." (p. 51).

All in all, the literature on the privacy paradox shows that discussions around it are still ongoing. While some scholars frame it through privacy calculus theory as context-sensitive trade-offs under bounded rationality, others demonstrate stable and structured preferences that challenge the paradox's very existence. Some authors go further in the debate and argue that the paradox is a conceptual misunderstanding stemming from the misalignment between general attitudes and specific behaviours. Overall, the research community faces significant hurdles in drawing conclusions, as authors frequently refer to different constructs (e.g., varying definitions of privacy concerns, disclosure behaviours, and risk perceptions) without a comprehensive explanation. Three critical limitations emerge: (1) methodological inconsistencies, (2) the

heterogeneity of studied data types (from demographic to behavioural data), and (3) the lack of a shared definition of core concepts. Notably, while consumers do engage in privacy trade-offs, they often lack the tools for well-considered, self-regulated decisions, suggesting that design solutions should adapt to diverse cognitive styles. Ultimately, the paradox appears more as conceptual, behavioural and methodological biases, underscoring the need for unified frameworks that capture how individuals actually value and protect privacy across digital contexts.

3 CONCLUSIONS

The examination of literature on data privacy through an economic lens reveals the challenges of valuating individuals' preferences and actual behaviours. Our analysis first establishes the background and context of the literature review by defining the terms and characteristics bounded to digital sovereignty, which has not been yet analysed at the individual level. In a second step, we demonstrated the role of contextual specificities, as well as of behavioural biases. These are for instance the high burden put on cognitive abilities that represents websites' and apps' terms and conditions, or psychological factors like the present bias that overemphasize immediate costs and benefits. These biases distort risk assessments in data privacy decisions, leading to frequent misalignment between stated preferences and actual behaviours, referred to as the privacy paradox. Our review of valuation techniques highlighted the predominance of studies based on the elicitation of willingness to pay (or willingness to accept compensation) for data disclosure, and therefore mainly relying on Discrete Choice Experiments or Contingent Valuation methods. Still, methodological gaps in measuring and modelling privacy aspects remain, with for instance the long-lasting debate on the choice between opting for WTP or WTA. Ultimately, the privacy paradox discussion stemming from the discrepancy between individuals' attitudes or concerns and intentions or behaviours exposes ongoing debates about the frameworks and conceptual definitions to adopt. Yet, seeing the privacy paradox as an economic trade-off seems to be more realistic, making therefore the theoretical approaches based on privacy-calculus best suited to the topic. Together, these findings suggest that current approaches to digital sovereignty must address three dimensions: (1) developing behavioural frameworks that account for cognitive limitations, (2) creating context-sensitive valuation methodologies, and (3) establishing reliable models to resolve validity issues. Digital sovereignty is not merely a technical or legal issue; it necessitates interdisciplinary solutions that connect human decision-making with systemic governance needs.

4 BIBLIOGRAPHY

Ackerman, M.S., Cranor, L.F., & Reagle, J. (1999). Privacy in e-commerce: examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, pp. 1-8. https://doi.org/10.1145/336992.336995

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), pp. 509-514. https://doi.org/10.1126/science.aaa1465

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age. *Journal of Consumer Psychology*, *30*(4), pp. 736-758. https://doi.org/10.1002/jcpy.1191

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research*, 49(2), pp. 160-174. https://doi.org/10.1509/jmr.09.0215

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), pp. 442-492. https://doi.org/10.1257/jel.54.2.442

Baldoni, R. (2025). *Sovranità Digitale: Cos'è e quali sono le Principali Minacce del Cyberspazio Nazionale*. Il Mulino. ISBN: 978-88-15-39238-1

Bansal, G., Zahedi, F.M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information & Management*, *53*(1), pp. 1-21. https://doi.org/10.1016/j.im.2015.08.001

Barth, S., & de Jong, M.D.T. (2017). The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, *34*(7), pp. 1038-1058. https://doi.org/10.1016/j.tele.2017.04.013

Blythe, J.M., Johnson, S.D., & Manning, M. (2020). What is security worth to consumers? Investigating willingness to pay for secure Internet of Things devices. *Crime Science*, *9*(1), pp. 1-9. https://doi.org/10.1186/s40163-019-0110-3

Chen, S., Gu, C., Wei, J., & Lv, M. (2023). Research on the influence mechanism of privacy invasion experiences with privacy protection intentions in social media contexts: Regulatory focus as the moderator. *Frontiers in Psychology*, *13*(1031592). https://doi.org/10.3389/fpsyg.2022.1031592

Cloos, J., & Mohr, S. (2022). Acceptance of data sharing in smartphone apps from key industries of the digital transformation: A representative population survey for Germany. *Technological Forecasting and Social Change*, *176*(121459). https://doi.org/10.1016/j.techfore.2021.121459

D'Annunzio, A., & Menichelli, E. (2022). A market for digital privacy: Consumers' willingness to trade personal data and money. *Economia e Politica Industriale: Journal of Industrial and Business Economics*, *49*(3), pp. 571-598. https://doi.org/10.1007/s40812-022-00221-5

European Commission. (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union* (COM/2010/0609 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52010DC0609

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, 77, pp. 226-261. https://doi.org/10.1016/j.cose.2018.04.002

Glasgow, G., Butler, S., & Iyengar, S. (2021). Survey response bias and the 'privacy paradox': Evidence from a discrete choice experiment. *Applied Economics Letters*, *28*(8), pp. 625-629. https://doi.org/10.1080/13504851.2020.1770183

Goad, D., Collins, A.T., & Gal, U. (2021). Privacy and the Internet of Things – An experiment in discrete choice. *Information & Management*, 58(2). https://doi.org/10.1016/j.im.2020.103292

Goldfarb, A., & Que, V.F. (2023). The economics of digital privacy. *Annual Review of Economics*, *15*(1), pp. 267-286. https://doi.org/10.1146/annurev-economics-082322-014346

Jensen, C., & Potts, C. (2004). Privacy policies as decision-making tools: an evaluation of online privacy notices. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*, pp. 471-478. https://doi.org/10.1145/985692.985752

John, L.K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of consumer research*, *37*(5), pp. 858-873. https://doi.org/10.1086/656423

Jung, W.-J., Shin, W., & Kim, H.-W. (2025). Estimating the monetary value of personal information on social networking sites. *Electronic Commerce Research*, *25*(2), pp. 1089-1114. https://doi.org/10.1007/s10660-023-09715-3

Kianpour, M., Kowalski, S. J., & Øverby, H. (2021). Systematically Understanding Cybersecurity Economics: A Survey. *Sustainability*, *13*(13677). https://doi.org/10.3390/su132413677

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, pp. 122-134. https://doi.org/10.1016/j.cose.2015.07.002

Madiega, T. (2020). *Digital Sovereignty for Europe* (PE 651.992). European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Malgieri, G., & Custers, B. (2017). Pricing Privacy – The Right to Know the Value of Your Personal Data. *Computer Law & Security Review*, 34, pp. 289-303. https://doi.org/10.1016/j.clsr.2017.08.006

OECD. (2013). *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value* [OECD Digital Economy Papers, No. 220]. https://doi.org/10.1787/5k486qtxldmq-en

Palazzo, C. (2016, 26 may). Consumer campaigners read terms and conditions of their mobile phone apps… all 250,00 words. *The Telegraph*. https://www.telegraph.co.uk/technology/2016/05/26/consumer-campaigners-read-terms-and-conditions-of-their-mobile-p/

Paliński, M. (2022). Paying with your data. Privacy tradeoffs in ride-hailing services. *Applied Economics Letters*, *29*(18), pp. 1719-1725. https://doi.org/10.1080/13504851.2021.1959891

Prince, J. T., & Wallsten, S. (2022). How much is privacy worth around the world and across platforms?. *Journal of Economics & Management Strategy*, *31*(4), pp. 841-861. https://doi.org/10.2139/ssrn.3528386

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). (2016). *Official Journal of the European Union*, L 119, pp. 1–88. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

Skatova, A., McDonald, R., Ma, S., & Maple, C. (2023). Unpacking privacy: Valuation of personal data protection. *PLoS ONE*, 18(5). https://doi.org/10.1371/journal.pone.0284581

Solove, D. J. (2021). The myth of the privacy paradox. *Geo. Wash. L. Rev.*, 89. https://doi.org/10.2139/ssrn.3536265

Stutzman, F.D., Gross, R., & Acquisti, A. (2013). Silent listeners: The evolution of privacy and disclosure on Facebook. *Journal of privacy and confidentiality*, 4(2), pp. 7-41. https://doi.org/10.29012/jpc.v4i2.620

van Ooijen, I., & Vrabec, H.U. (2019). Does the GDPR Enhance Consumers' Control over Personal Data? An Analysis from a Behavioural Perspective. *Journal of Consumer Policy*, *42*(1), pp. 91-107. https://doi.org/10.1007/s10603-018-9399-7

Wein, T. (2022). Data Protection, Cookie Consent, and Prices. *Economies*, 10(12).https://doi.org/10.3390/economies10120307

Winegar, A.G., & Sunstein, C.R. (2019). How Much Is Data Privacy Worth? A Preliminary Investigation. *Journal of Consumer Policy*, *42*(3), pp. 425-440. https://doi.org/10.1007/s10603-019-09419-y

Wottrich, V.M., Van Reijmersdal, E.A., & Smit, E.G. (2018). The privacy trade-off for mobile app downloads : The roles of app value, intrusiveness, and privacy concerns. *Decision Support Systems*, 106, pp. 44-52. https://doi.org/10.1016/j.dss.2017.12.003

Yamaguchi, S., Oshima, H., Saso, H., & Aoki, S. (2020). How Do People Value Data Utilization?: An Empirical Analysis Using Contingent Valuation Method in Japan. *Technology in Society*, *62*(101285). https://doi.org/10.1016/j.techsoc.2020.101285

Zamparini, L. (2024). Data, digital markets, and the economic value of privacy. *Eastern Journal of European Studies*, *15*(2), pp. 147-164. https://doi.org/10.47743/ejes-2024-0208