van Zeeland and Pierson
Financial Innovation (2024) 10:29
https://doi.org/10.1186/s40854-023-00533-y

Financial Innovation

RESEARCH Open Access

Changing the whole game: effects of the COVID-19 pandemic's accelerated digitalization on European bank staff's data protection capabilities

Ine van Zeeland[1*] and Jo Pierson[2]

*Correspondence:
ine.van.zeeland@vub.be

[1] Imec-SMIT (Studies on Media, Innovation and Technology), Faculty of Social Sciences and Solvay Business School, Vrije Universiteit Brussel, Pleinlaan 9, 1050 Brussels, Belgium
[2] Faculty School of Social Sciences, Hasselt University, Kantoor FR-4.1 Faculteit Rechten Gebouw, Martelarenlaan 42, Hasselt, Belgium

Abstract

The COVID-19 pandemic accelerated the acceptance of digital banking services such as online payment and banking apps. As bank clients become more likely to use online services and contactless payment, the amount of consumer data available for banks' digitalization strategies has increased. This acceleration in digital banking has placed a spotlight on retail banks' efforts to protect personal data. Bank staff are on the front-lines of both protecting personal data and communicating their banks' efforts in this respect to maintain consumer trust. Our study aimed to answer the following question: How did the sudden increase in digitalization during the pandemic affect bank staff's capabilities in protecting personal data? In a two-stage qualitative study, we collected empirical data on bank staff's data protection efforts during accelerated digitalization. Analyzing our findings from the perspective of technological mediation theory, which focuses on the relationships between technologies, practices, and social arrangements, we found that in banking platformization, bank staff are disempowered in supporting clients, who are responsibilized for protecting themselves from fraud. Competitive pressures push retail banks into using client data in ways beyond sector norms, endangering the contextual integrity of data flows. Further, our findings show that digitalization presents bank clients with new risks, of which they are informed only after changing their banking practices, and it may be difficult to return to former arrangements. The application of mediation theory, combined with contextual integrity theory, clarified the shifting positions of different digital technology users in the infrastructural network of platformized banking and allowed for an in-depth analysis of conflicting interests. By clarifying these interests, difficulties were identified that need to be addressed in public policy and digital innovation projects to prevent loss of trust among bank clients.

Keywords: Digitalization, Pandemic, Banks, Privacy and data protection, Bank staff

Introduction

As a consequence of the 2008 credit crisis, the banking sector has been at the vanguard of digital transformation to cut costs and improve efficiency (Kou et al. 2021). The low interest rates that governments and central banks introduced as a crisis response spurred the rise of the digital economy (Srnicek 2017; Broby 2021). As low interest rates and declining profitability endured for over a decade, banks sought other sources of revenue through new services and partners and by monetizing data (Broby 2021; Chen et al. 2017). In addition to cost reduction and capitalizing on data collection, banks set up digital platforms to meet clients' evolving needs for online services (Swacha-Lech 2017; Kou et al. 2021), and in Europe, to comply with Open Banking legislation (Colangelo and Maggialino 2019). Hendrikse et al. (2018) describe this development as the "Appleization of finance," that is, mimicking successful technology companies' strategies by developing integrated banking platforms, with the goal of locking in customers.

However, before 2020, European consumers were slow to adopt platformized (retail) banking. The European Central Bank (2020) reported that, in 2019, 73% of payments were still made in cash, and while apps were the dominant channel through which European clients engaged with their banks (CB Insights 2018), ING Bank found in a survey conducted in 2019 that only 30% of their European clients felt comfortable sharing financial data with other organizations (Exton 2020). This highlights the connection between sharing financial data and trust. Client trust and trustworthiness are highly relevant to the acceptance of data-intensive innovation in the financial sector (Aitken et al. 2020).

When the COVID-19 pandemic began, many countries introduced social distancing measures. Consequently, as bank clients became much more inclined to use online services and contactless payment methods, the development of online banking services accelerated (e.g., Baicu et al. 2020; Haapio et al. 2021; Hemachandra and Sharkasi 2021; Kitsios et al. 2021). Average weekly hours spent on finance apps instantly increased worldwide after lockdowns were announced in March 2020 (App Annie 2020). Fear of contagion and pandemic-induced lifestyle changes dramatically increased the use of cashless payments in 22 countries (Wisniewski et al. 2021). This disruptive effect of the COVID-19 crisis increased the amount of digital transaction data available to banks for developing digitalization strategies (Maiti et al. 2021), changing their priorities (Fiserv 2020) and increasing market orientation (Haapio et al. 2021). We refer to this effect of the pandemic on the adoption of digital retail banking services and strategies as "accelerated digitalization."

The acceleration of the digitalization of services resulting from the COVID-19 pandemic places the effects of digitalization in a stark light. A marked uptick in the use of digital services raises questions about gaps in skills and knowledge in both the wider population and those providing these services (FSB 2022). Digitalization transforms the retail banking experience for all actors involved: clients, bank staff, regulators, financial technology (FinTech) providers, and new entrants in open banking such as retailers and large platform providers ("Big Tech"). Digital technologies are rapidly changing our environment, and all users are transformed by and with them (Verbeek 2015), needing to adapt their practices and learn new skills (Lievrouw 2014). Previous studies have focused on adaptations on the side of FinTechs (Carbó-Valverde et al. 2022; Li and Xu 2021; Romānova et al. 2018), regulators (Leong 2020; Nicholls

2019; Remolina 2019), consumers (Baicu et al. 2020; Reynolds 2017; Van Der Cruijsen 2020), or other users of open banking services (Irimia-Diéguez et al. 2023; Yao and Li 2022); however, this study centers on the adaptations of bank staff. In particular, this study focuses on bank staff's capabilities to protect clients' personal data as an important element in establishing trust in financial data sharing.

In a 2021 report, the European Banking Authority (EBA) highlighted several new risks resulting from the platformization of banking: misuse of personal financial data, digital profiling, cybercrime, and risks arising from overly complex digital assets and services. These risks highlight the need to promote digital financial literacy (EBA 2021). Bank staff potentially have an important role to play as the frontline in protecting personal data, promoting clients' digital financial literacy, and communicating banks' efforts in this field to maintain consumer trust.

Protecting personal data is also a transnational legal requirement in the European Union (EU). The right to protection of personal data in the EU refers to the protection of the "fundamental rights and freedoms of natural persons," as the General Data Protection Regulation (GDPR) states (Article 1(2)). These fundamental rights and freedoms include the right to privacy, the protection of personal data, non-discrimination, and other rights and freedoms specified in the European Convention on Human Rights and the EU Charter of Fundamental Rights.

Payment data may reveal employment information, religious affiliation, union membership, sexual preferences, health issues, and other potentially sensitive elements of people's lives. This makes payment data valuable for various parties in the digital economy, as a myriad of conclusions can be drawn about consumer behavior (Westermeier 2020), providing new opportunities for targeted advertising or commercial surveillance (O'Dwyer 2015). However, more extensive use and sharing of such data also creates risks to people's rights and freedoms that are covered under the "right to protection of personal data" (Ferrari 2020).

Based on the above, we address the following research question in this study: How did the accelerated digitalization of banking during the pandemic affect the capabilities of bank staff's in protecting personal data? Our interest is both theory- and literature-driven, grounded in theories of technological mediation (e.g., Latour 1992; Verbeek 2005; Lievrouw 2009) and privacy as contextual integrity (Nissenbaum 2004, 2010). Mediation theory predicts that, as digital technologies assume a more prominent position in banking, the practices of all actors in the banking system must be adapted, and new arrangements made for society and institutions. This research focuses on the data protection practices of bank professionals; however, these practices are intertwined with the context in which these professionals work, other human actors, and technologies in the system.

To explore the real-world practices of bank employees regarding the protection of personal data, we conducted empirical research aimed at uncovering practitioners' views, priorities, and interpretations in rich detail. To this end, we conducted a qualitative study in two stages: gathering expert opinions on the main challenges to the protection of personal data in digital banking in the first stage, followed by fieldwork in the European banking sector in the second stage, including observations in a large

European Global Systemically Important Bank (G-SIB), interviews with professionals, and expert panel discussions.

Our findings show that the platformization of banking changes practices and reorders the capabilities of different actors in the system, including new actors. Accelerated digitalization displaces certain data protection risks from retail banks to clients who struggle to protect themselves from confidence schemes, such as phishing and online scams. Moreover, during the pandemic it became clear that bank staff lack sufficient digital skills and strategic insights to adapt to the impact of infrastructural innovation on their practices. As this could undermine the public's trust in digital financial services, stronger enforcement of transparency requirements regarding digital banking risks is needed. In addition, more extensive digital skills training for bank staff is advised, both to foster strategic thinking regarding digitalization and raise awareness of risks to personal data in digital services.

The remainder of this paper is organized as follows. In the "Theoretical background" section, we introduce the theory of technological mediation, the theory of contextual integrity, and perspectives from infrastructure and platform studies. The methodology of our study is described in the "Methodology" section, and our findings are presented in the "Findings" section. In the "Limitations" section, we clarify the limitations of our research approach before discussing our findings in light of the theoretical framework in the "Discussion" section. Finally, the "Conclusion" section presents our conclusions.

Theoretical background

In this section, we first review key theories of technological mediation and contextual integrity, connecting them to the banking sector, followed by the literature and previous research on platformization and the effects of infrastructural changes on social arrangements related to retail banking.

Mediation theory

We are concerned with the consequences of accelerated digitalization for retail banking staff's capabilities to protect personal data; therefore, we begin by considering a prominent theoretical perspective on the role of digital technologies in society: the theory of (technical or technological) mediation, also known as mediation theory. Mediation theory has taken root in the academic disciplines of science and technology studies (STS), philosophy of technology, and media and communication studies (MCS). Although these disciplines differ in the academic backgrounds that have led to their perspectives on technological mediation, they converge on the notion that technology influences how humans interpret reality and act, while humans steer technological design, in an entanglement of mutual influence ("mutual shaping").

Within STS, it is a given that technologies are designed by people, and that the technology design process, while seemingly focused on effectiveness and efficiency, is far from being free of social and political considerations (Winner 1980; Pinch and Bijker 1984). For instance, market pressures drive researchers to pursue commercially profitable paths of inquiry rather than less commercially attractive alternatives (Benanav 2020). Moreover, researchers depend on and are accountable to funders, policymakers, regulators, their scientific networks, and wider society; thus, they actively seek to work

with the confirmation biases they assume these stakeholders hold, to have the "facts" they construct accepted (Latour and Woolgar 1979). Whether intentionally or inadvertently, researchers and developers often entrench the existing social order in the technologies they design, although they may also reorder power (Winner 1980). For example, the infrastructure of international finance still reflects a colonial background, whereas the communications infrastructure of the Society for Worldwide Interbank Financial Telecommunications (SWIFT) has been repeatedly drawn into global security politics (Dörry et al. 2018; De Goede 2020; Scott 2022).

Within this perspective on technology design, also known as "the social construction of technology" (SCOT), technologies are constructs that reflect the visions, political and social interests, and assumptions of their designers, the companies that employ those designers, their users, and the wider society in which they are made and used (Pinch and Bijker 1984). Technologies are "part of a long chain of people, products, tools, machines, money, and so forth," and embody "relations between heterogeneous elements" (Akrich 1992: 205). Therefore, technologies are neither neutral nor objective; they steer us, in the sense that they privilege certain social orderings: "technology is society made durable" (Latour 1990).

Latour (1990, 1992, 1993, 1999) notes that technological artifacts may or may not cooperate in the achievement of human goals, arguing that the things we encounter in reality can be helpful, counterproductive, or indifferent to our purposes. His "actor-network theory" presents human actors and artifacts as nodes in networks, that together produce more or less successful systems. A concrete example is the hybrid of human and technology constituted by a person with a smartphone, in which the hybrid has more capabilities than the person and smartphone each have separately. The human actors and artifacts—"actants" arising from the network that brings them together—influence each other and the relationships between them. Thus, according to Latour's views, we should study a system's human and non-human actants on an equal footing.

The combined human intentions and technological functions in a network "compose" new "programs of action," in which human intentions are "translated" by the additional capabilities technology affords (Latour 1993). Thus, translation and composition are two types of technological mediation. Two other types are "black-boxing" and "delegation."

Black-boxing is "a process that makes the joint production of actors and artifacts entirely opaque" (Latour 1999). For example, the Internet is a giant hybrid network consisting of nodes such as engineers, software developers, various devices, submarine cables, protocols, standards, and different types of users; however, we simply experience it as "the Internet" and interact with it while largely unaware of its complex composition. The complete network is black-boxed for most users, especially as long as it works. However, Latour argues that black-boxing is "reversible," because it is possible for the system to become visible for us. This occurs when a system stops functioning, and we become aware of its components and what is needed to make the system work again.

Delegation occurs in the design of technologies. Technologies can be delegated programs of action, such as in the case of automatic sliding doors. The way automatic doors function (e.g., how rapidly their sensors will notice your approach) co-shapes your behavior such as walking speed. Borrowing a term from Akrich (1992), Latour (1993) states that designers "inscribe" programs of action in technologies, which in turn have

"prescriptions" for their use. A technology's prescriptions make up its "script." As automatic doors have a script for how to use them, so do other technologies for their usage and what they will and will not allow. To some extent, technologies determine how and for what purpose they are to be used, and by whom.

Building on Latour and others (particularly Ihde 1990), the philosopher Verbeek (2005) argues that technologies transform and co-shape human experience. We experience reality through the technologies that we use, and they transform what we perceive. For example, when radiology makes an internal body part visible in a medical image, that image is co-shaped by the internal body part, the technology used to create the image (with specific capabilities and limitations), and the interpretation of an (un) trained observer. Seeing such medical images not only enhances human perception but also prompts new questions on how to act.

A key element of Verbeek's (2005) approach that influences our empirical analysis, is that technological mediation arises in specific use contexts. Consequently, how technological mediation occurs depends on the context. For example, technological mediation will differ between a medical setting and a retail banking setting. Many of the technologies themselves obviously differ between medical and banking contexts; however, even if they remain largely the same, such as health-monitoring apps and banking apps, the different contexts in which they are used mean that they differ in how they mediate our reality.

This is consistent with the privacy theory of contextual integrity, which holds that our sense of privacy is related to how appropriate the flow of information is in a given context (Nissenbaum 2004). Information flows are appropriate when they conform to context-specific informational norms. In contrast, privacy is breached when information flows do not conform to contextual norms. Rather than classifying certain types of data as high-risk or sensitive, contextual integrity theory holds that it is neither inherently wrong nor inappropriate to gather or use data about a person, nor does sharing personal information come with inherent harm, if the data are used or shared in line with context-appropriate purposes, values, and functions, as recognized by all actors in the context (Nissenbaum 2010).

Combining contextual integrity theory with mediation theory, we can surmise that, while certain ways in which technologies shape practices may be appropriate in one context, they may be inappropriate in other contexts, thereby violating people's sense of privacy. For example, although such behavior is not uncommon in other data-intensive industries, retail banks refrain from directly selling clients' digital transaction or in-app behavior data, as doing so may pose a reputational risk to banks, assuming that selling personal financial data does not conform to their clients' contextual norms (Van Zeeland and Pierson 2021).

The theory of technological mediation has also taken hold in media and communication studies (MCS), which has traditionally focused on how media influence society. MCS scholars have analyzed how media change communication and vice versa, and how mediated communication changes society and vice versa (Couldry and Hepp 2013). As a communication process, mediation changes the social environment (Dourish 2004; Silverstone 2005). Media technologies, such as the Internet, smartphones, and voice assistants, have become our social environment, and we are transformed by and with them.

Lievrouw (2014) describes mediation as mutually determining relationships among artifacts, practices, and arrangements (society and institutions). Technological mediation is expressed in the reconfiguration of communication abilities, remediation of practices, and reformation of social arrangements. A shift in artifacts, practices, or social arrangements will lead to shifts in the other two. For example, the Internet has fundamentally altered the nature of banking, changing banking services and practices, which, in turn, means that banking institutions must adapt (Broby 2021). Similarly, the introduction of smartphone apps for banking has led to new practices (banking-on-the-go, rather than in-person visits to bank branches) and social arrangements around banking (e.g., fewer physical branches). However, a change in social arrangements instigated by the pandemic has led to a need for socially distanced banking practices and digital banking services (Liébana-Cabanillas et al. 2022).

Infrastructure studies and platform studies

Digitalization of banking services transforms these services in many ways. Financial institutions' organizational processes, structures, and behaviors become fundamentally different when transformed into digital shapes (Chen et al. 2017). For instance, FinTech innovation may reduce the number of employees in traditional banks by approximately one-third (Citi GPS 2016). The number of bank branches in the United Kingdom (UK) was roughly halved between 1986–2014 (Bennett 2020), and a monthly average of approximately 54 bank branches have since been closed (Which? Money 2023). Thus, banking digitalization has consequences for the entire infrastructure.

The field of infrastructure studies (emerging from STS) comprises an extensive body of research on the features of ubiquity, reliability, and invisibility for infrastructures, and their functioning as gateways (Plantin et al. 2018). As users become habituated to a technological environment, its ubiquity, reliability, and durability lead them to depend on it. Financial infrastructures are deeply embedded in everyday life and are considered "critical infrastructures" in most countries (Westermeier 2020). Users have developed practices around them that sustain and increase interdependencies (Edwards et al. 2007). For example, in Western countries, employers generally expect employees to have bank accounts, as do tax authorities and retailers, among others.

Infrastructures are mostly invisible, "black-boxed," underlying networks. An example is the SWIFT network, which provides secure bank-to-bank messaging and handles approximately 80% of the global payment traffic, thus enabling and shaping important payment networks (Dörry et al. 2018). Its black-boxed nature is reversable, such as when it is used to exercise political power, as exemplified by the March 2022 disconnection of several Russian and Belarussian financial institutions from SWIFT, instigated by the EU, the United Kingdom (UK), Canada, and the United States (US), in response to the Russian invasion of Ukraine.

When discussing the digital transformation of the banking infrastructure, the human aspects should not be overlooked, not only in terms of job losses but also in terms of how functions and skill sets change and which roles humans will play in the new digital infrastructure. Ghosh and O'Neill (2020) argue that focusing on the platformization of mobile money systems leads us to overlook the human work that goes into making platforms work seamlessly in practice. An important element of making a digital system

work is whether the people who work with or are part of the digitalized process have the required digital skills (Mariën et al. 2017; Kitsios et al. 2021).

When existing networks need to incorporate more actors, other systems and new devices, standards, and routines must be explicitly redesigned. Currently, this is taking place in financial infrastructure as a consequence of digital transformation. This transformation is not an impersonal phenomenon; people are actively involved in creating it, from designing the application programming interfaces (APIs) and developing open banking policies, to choosing contactless payment methods instead of using cash. The sociotechnical infrastructure of digital banking consists not only of institutions and technologies but also of people's daily practices and habits. An important element of digital transformation is the "platformization of banking" (Hendrikse et al. 2018; Westermeier 2020) driven by regulatory demands, such as the EU's revised Payment Services Directive (PSD2) and the UK's Open Banking (constituting a change in social arrangements), making it valuable to study these current developments from a platform studies perspective.

The field of platform studies (emerging from MCS) analyzes platforms' affordances and constraints, while also examining the ways in which platforms connect heterogeneous actors (Plantin et al. 2018). The key points of interest are the accessibility of data through platforms and the logic imposed by APIs. The most important characteristics of platforms are that they position themselves (a) between users (consumers, third-party providers, or even physical objects) and (b) as the ground upon which users' activities occur (Srnicek 2017). The latter characteristic provides platforms privileged access to those activities and the power to set rules and shape markets, even if a platform presents itself as neutral (Gillespie 2010). In the case of banking platforms, banks can potentially gather a wide variety of data on all users (Westermeier 2020), including not only bank clients but also other service providers, and all these data can be mined for insights that can be monetized or used to improve services.

Platformization offers banks distinct advantages in offering innovative services. Although incumbent banks also strive for innovation in-house, they mostly acquire innovative services from FinTech start-ups (Hendrikse et al. 2018). Through platforms, incumbent banks can benefit from innovation by externalizing risk-taking and development costs without heavy disruption to the ecosystem they dominate (Hendrikse et al. 2018). Meanwhile, FinTech start-ups can cultivate a business model that strives to be acquired by or collaborate with banks as established, affluent partners who already have a large group of clients (Valero et al. 2020).

In banking platformization, consumer interaction with finances in digital environments, such as websites and apps, is designed along the lines of user experience design trends to provide an "'intuitive" user interface that has little in common with physically visiting a bank branch (Dieter and Tkacz 2020). As people adapt their lives to rely on digital banking, and banking platforms adapt to clients' usage patterns in data-driven design, this mutual shaping may mean that eventually, people cannot return to offline banking, as their habits and societal practices become entangled with technology (Orlikowski and Scott 2008).

The COVID-19 crisis has been highly disruptive to the digital banking system, providing a prime opportunity to analyze how this sociotechnical system functions, as

disruptions create situations in which black-boxing is reversible, bringing the underlying structures and arrangements to the surface. In examining how banking staff protect personal data in practice and how their roles change in times of accelerated digitalization, perspectives from infrastructure and platform studies provide key insights for our empirical analysis. The theory of technological mediation underpinning these perspectives highlights digital banking's reconfiguration of communication abilities, remediation of practices, and reformation of social arrangements.

Considering the protection of personal data in retail banks as a matter of contextual integrity brings necessary nuance to the discussion of platformized or "open" banking. Context matters in a comprehensive analysis of the effects of digitalization on practices and arrangements, as does the insight that context-specific practices and arrangements also affect digitalization. Thus, how accelerated digitalization affects bank employees' ability to protect clients' personal data may have more complex explanations than the one-dimensional focus on the effects of introducing digital technologies would provide.

Methodology

The main research question we aimed to answer is as follows: How did the sudden increase in banking digitalization during the pandemic affect bank staff's capabilities in protecting personal data? We conducted a qualitative empirical study throughout 2020 and during the first half of 2021. The interplay of factors that influence the practice of data protection is a complex, context-specific phenomenon that calls for detailed exploration. Therefore, our research strategy was designed to collect so-called "thick" descriptions, reflecting the richness and diversity of practitioners' views, priorities, and practices to identify what they regard to be crucial factors. Rather than aiming for expert consensus on preset alternative outcomes (e.g., Chao et al. 2021), we follow the recommendations of Meuser and Nagel (2009) to the effect that experts reveal most about their values and interpretations and what they consider to be relevant and meaningful when allowed to talk freely. For this purpose, an immersive study was conducted, involving expert discussions, observational field research at the Brussels hub of a G-SIB, 35 interviews with experts from various countries, international panel discussions, and document analysis.

We designed this study to identify the practical challenges that banks face in protecting personal data in the context of rapidly evolving technological innovation. The study design comprises two steps:

1. An exploratory focus group ("roundtable") discussion with various stakeholders from the financial sector to identify important practical challenges to personal data protection; and
2. Fieldwork within a major bank to explore those challenges in practice, supplemented with interviews and panel discussions with experts from different countries, both inside and outside Europe.

The exploratory roundtable discussion with experts was conducted in September 2019. It consisted of a 2-h discussion with expert participants selected to represent different stakeholder groups in the banking sector. The 13 participants represented leading banks,

academia, a banking industry alliance, a pan-European consumer alliance, a financial consultancy, and a FinTech industry alliance, and one participant worked for a (national supervisory) Data Protection Authority until a few months prior to the discussion.

The discussion followed the lines of a World Café focus group, which facilitates the elicitation of important themes on a specified topic from a heterogeneous group of participants (Brown and Isaacs 2005; Löhr et al. 2020). In three rounds lasting 30 min each, mixed subgroups of four to five participants discussed their views on the major challenges to the sector in relation to personal data protection (round 1) and potential or practical solutions to those challenges (round 2), after which they evaluated the challenges and solutions identified by the other groups (round 3). The discussion concluded with a group-wide discussion of the main takeaways. A report on the discussion was published and circulated among the participants and other industry experts to verify the validity of the findings, which yielded nothing but confirmations.

The main challenges to the protection of personal data in the banking sector identified in the discussion are as follows:

- the transparency paradox (what is understandable and sufficient information for clients regarding the processing of personal data),
- competitive pressure from challengers that have more personal data (specifically "Big Tech" companies),
- conflicting regulations around personal data protection, and
- automated creditworthiness assessments (what are acceptable considerations, and can these assessments still be explained).

The identification of these challenges guided the subsequent fieldwork, and the main challenges were used as focal points in analyzing observations and desk research and as questions in semi-structured interviews conducted alongside the field research (see Additional file 1 for interview protocols). Nevertheless. The field work, interviews, panel discussions, and document analysis remained open to unexplored "emerging" themes as they presented themselves during the period (Daynes and Williams 2018).

The second step of the study consisted of ethnographic observations in a G-SIB, as well as interviews and discussions with industry experts beyond this bank. The observational study was preceded by a conference panel discussion in January 2020 with an audience (academic, regulatory, and professional experts) on the topic of personal data protection and PSD2.

When lockdown measures were introduced in March 2020, the bank's staff were no longer meeting colleagues or clients in-person. Gradually, as people became habituated to working online and meeting virtually, the pandemic effectively replaced "co-location" with "co-presence" in a digital environment (Howlett 2021).

The researchers followed the field online using a "digital ethnography" approach. Digital ethnography acknowledges that our reality is increasingly entangled with digital "technologies, content, presence, and communication." while "the digital has become part of the material, sensory, and social worlds we inhabit" (Pink et al. 2015: 2, 7). The pandemic measures meant that "being there" in the field effectively meant "being online." Work floor observation turned into online meeting attendance, remote access

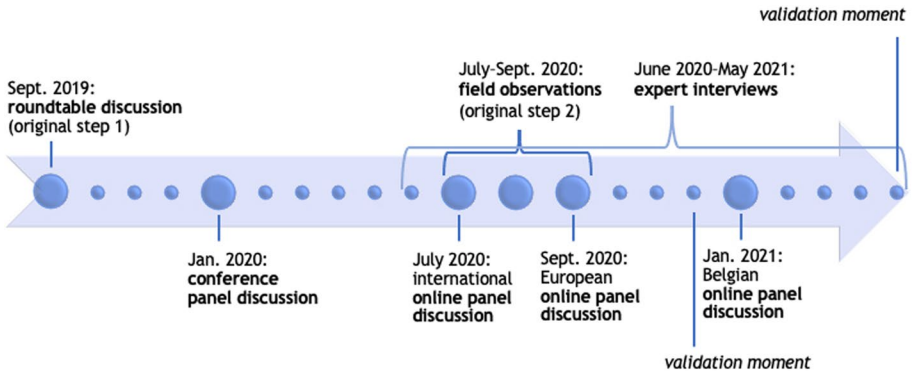

Fig. 1 Timeline of methodological steps

to documentation, and in-depth interviews. Figure 1 presents the timeline of the study's methodological steps.

Three interviews were held in-person, two were held over the telephone, and 20 interviews were held online using videoconferencing tools. The 25 expert interviews were semi-structured (see Additional file 1 for the interview protocols) and lasted approximately one hour each. The fact that people became more habituated to interacting online, or being co-present in a digital environment, provided the additional benefit of being able to interview experts who were physically located further abroad (Belgium, France, and South Africa) without substantial technical support.

The same was true for three additional online panel discussions among experts from around the world, the EU, and Belgium, respectively. The panels discussed topics that emerged from our observations and interviews in the second part of the study: open banking, PSD2, and data-sharing between banks and government authorities for purposes of public interest. These two-hour online discussions also functioned as focus groups, exploring "attitudes and perceptions, feelings and ideas," to gauge "the extent to which there are shared views among a group of people in relation to a specific topic" (Denscombe 2014). The experts in our panels and interviews were (G-SIB) bank executives and board members, (financial) technology and innovation specialists, data protection officers, legal specialists, data governance specialists, auditors, client-facing bank staff, consumer association representatives, representatives of regulatory and government authorities, and consultants.

As the regular interactions between banking professionals themselves also mostly took place through videoconferencing, we attended online meetings, industry workshops, and conferences to observe professional discussions. Thus, we participated in various work meetings, ranging from biweekly discussions on data protection issues to API assessments, and attended dozens of industry webinars.

When COVID-19 crisis measures eased somewhat at the end of June 2020, the first author was also able to spend three times five days on the work floor (15 non-consecutive work days), as teams were allowed back into the office in three-week rotations. Additionally, we analyzed internal and public documentation on the topic of personal data protection in the banking sector, including industry reports, audit reviews, planning documents, newspaper articles and opinion pieces, and presentations to the board of a bank. This documentation was collected between September 2019 and May 2021.

Thus, the empirical data collected consisted of interviews, panel transcripts, digital documents, and thousands of field notes. These were systematically analyzed using a qualitative coding method and data analysis software (MaxQDA), to iteratively develop emergent "codes" into themes and identify patterns and concepts (Daynes and Williams 2018). Our interview and panel results were triangulated using documents and observations, and the findings were checked and validated in presentations and feedback sessions with banking professionals, including some of our respondents. Given that this was an exploratory study with a relatively select sample of respondents, we refrained from drawing quantitative conclusions.

Findings

In this section, we discuss the effects of accelerated digitalization induced by the COVID-19 pandemic on bank staff and their interaction with clients, to the extent that they are involved in the protection of personal data. We begin by presenting our findings related to the main challenges identified by the expert roundtable participants during the first stage of our research. We also discuss another theme that emerged through our analysis: the (lack of) digital skills and data protection awareness among both bank employees and clients, which is of some concern because of the important communicative role that bank staff play in protecting personal data.

The transparency paradox

Transparency on personal data processing is an important requirement in data protection legislation, including "notice and consent" regimes and the EU's GDPR. Figure 2 provides a (simplified) overview of the transparency requirements in the GDPR.

GDPR Article 5 (1)(a) states that transparency is a basic principle of personal data protection, which relates to, at minimum, the provision of information to the data subjects for the purposes of processing personal data and the identity of the controller (the entity deciding on the purposes and means of data processing). It requires that "any information and communication relating to the processing of […] personal data be easily accessible and easy to understand, and that clear and plain language be used" (Recital 39). People "should be made aware of risks, rules, safeguards, and rights in relation to the processing of personal data and how to exercise their rights" (Recital 39), and "any information addressed to the public or to the data subject [should] be concise, easily accessible and easy to understand" (Recital 58).

Other stipulations of the GDPR (most notably, Articles 12–14) also require information be provided on risks and safeguards and data processing in specific circumstances, such as whether personal data will be shared with other recipients, transferred to non-EU countries, or used for automated decision-making. In the latter case, "meaningful information" should be provided about "the logic involved" (Article 13 (3)(f)). In brief, tension clearly exists between the amount and type of information to be provided and requirements that such information be concise and intelligible.

In our exploratory roundtable discussion, one participant described this "transparency paradox" as follows: "What is the level of transparency and consent that the client can really handle? What does the consumer want, and when do you start to annoy

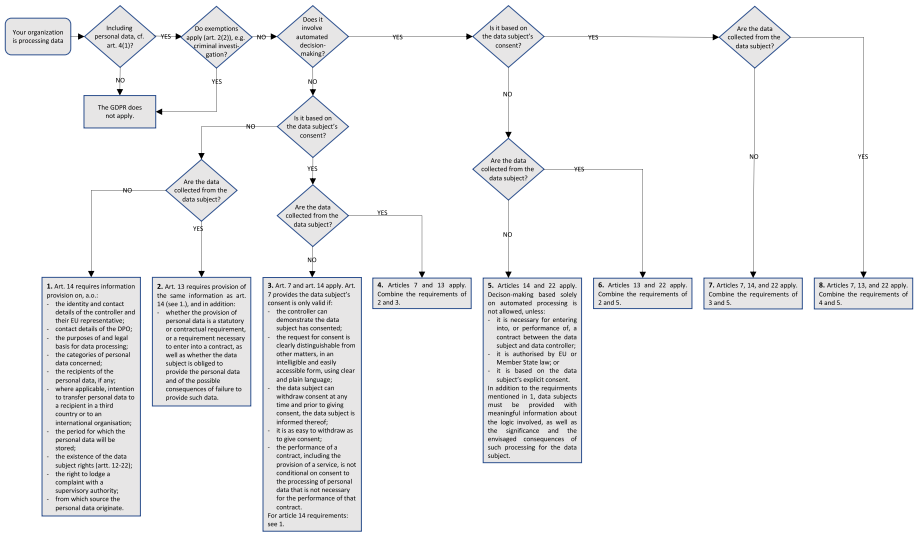

Fig. 2 A simplified overview of GDPR transparency requirements

them?" Similarly, a banking innovation expert remarked in an interview: "The thing with explaining is that it is like the cookie consent, terms and conditions—all these explainers are in your way. Explaining stuff to customers requires that they want to know and are open to hearing it here and now."

During the roundtable discussion, the experts emphasized that consumers are more sensitive about financial information than other types of data, with one participant remarking that people tend to read information about their financial data three times. While the GDPR requires transparency in all cases of personal data processing, it is particularly pertinent when bank clients are asked to provide their consent, as a consent request is not valid if information is incorrect or incomplete, or if there is no option to decline. The roundtable experts highlighted the importance of consumer trust to banks, which means "softening" consent requirements (e.g., remaining vague about purposes or risks) to make it easier to use data would not be a long-term solution for banks.

Referring to the platformization of banking in particular, a banking expert from a pan-European consumer advocacy group remarked during our conference panel discussion: "It is very difficult for the consumer to actually understand what is going on, to give meaningful consent. Also, I must say that there are lots of parties out there that don't make it easier for the consumer, when you look at how certain interfaces are designed, for example. Everything seems to be designed somehow to get from the consumer what you would like to get from the consumer." He further added: "The burden shouldn't be always only on the side of the consumer. These are very complex issues and complex activities that are going on and different parties involved. […] I think that we also need to make it easier for the consumers in terms of how everything is designed and the whole issues about the settings, and the privacy-by-design obligations are very important."

The roundtable experts acknowledged that transparency requirements can inspire ethical behavior. Specifically, if a financial organization needs to be transparent about the characteristics of the people used in profiling, it will think twice about the relevance of certain characteristics. However, automated decision-making and the data

on which it is based reflects the core business of the financial sector; having the right data and analyzing it in the right way provides a competitive edge. Thus, providing excessive explanations can be detrimental to a bank's core business.

Despite the transparency requirements described above, EU banks tend to emphasize positive benefits rather than risks or rights in their communication regarding how personal data is handled in digital banking. An open API specialist at a German G-SIB stated the following during an industry webinar: "We don't talk with our customers about open banking and PSD2 there. We don't do that. The only thing that we tell our customers is the value proposition and what is the value that they can get in case that they, for example, get if we aggregate data. So, it all comes back to the real benefit and real value for the customers."

In the same webinar, an open banking specialist from a Dutch G-SIB stated: "I think it is also for us as banks to take up this educational role towards our clients and really empower them, by really making them understand the power of their own data. So, everything they do: the movement of a mouse on the screen and the moment of that doing so, and how you entitle or name your email address, and so there are a lot of digital behaviors in this completely digital world that we act in, that really define digital profiles of you." An innovation expert at the (French) G-SIB where we conducted our observations, voiced a similar reflection: "We could start building some education that could position a bank as a party that keeps your data safe. [Clients would then] understand better why we are more valuable for them. From a marketing perspective, this could be interesting indeed. […] They do see the value of 'we're not letting your money slip out of your account,' but they don't see the same benefit for their data."

Regarding the effects of the COVID-19 pandemic on transparency and communication, experiences with remote working were very relevant. A business development expert at a "Big Tech" company remarked during the Belgian Digital Finance Summit 2020: "We've seen a drastic change in the behaviors of the banks. […] Think about a bank traditionally servicing their clients in the branch office, and all of a sudden, they need to do it remotely, over video conferencing. Also for signing paperwork. This has clearly highlighted the importance of the human factor in this digital transformation, and the need for a cultural transformation."

In an internal webinar on the future of retail banking, a senior manager within the G-SIB where we conducted our observations envisioned a change in the banker–client relationship to hybrid online–offline interactions at "virtual branches." In another internal webinar, a C-level manager remarked that "the COVID crisis has had a big impact on our clients, but it has improved our relationship with our clients tremendously; we have never before communicated this much with our clients" (a clear "reconfiguration of abilities to communicate"), and noted that private banking advisers would be retrained in digital skills, such as giving online presentations.

Client-facing staff generally reported positive responses to how the changes in arrangements during the pandemic necessitated new practices: clients were accepting of the extraordinary circumstances and willing to interact online to avoid the health risks of physical meetings. A home loan adviser who expected to need to overcome resistance in clients in discussing a major life event, such as buying a house online,

was happily surprised at how smoothly interacting over videoconferencing tools was accepted.

New data protection-related practices prompted by the pandemic appeared on the outside to be mainly related to digital security. Online interactions require automated security measures and access restrictions to protect privacy and personal data, allowing for little flexibility. Clients calling or emailing to request information about their personal finances first needed to be digitally authenticated over a secure connection, which was experienced as more complicated than authentication for in-person interactions.

Despite these efforts, digital fraud and phishing have soared to unprecedented heights since the start of the COVID-19 crisis (Al-Qahtani and Cresci 2022). During the first pandemic wave (March–June 2020), bank staff reported seeing approximately 150 online fraud cases detected per day. While authorities called on banks to become more proactive in educating and protecting their clients, and bank communications issued warnings about fraudulent tactics and continually stressed caution in sharing security codes, bank staff felt unable to help clients who had already fallen into a phishing trap, which became increasingly common. One employee explained, "When it comes to phishing and such, we as client advisors cannot do much about it, because it is the client who has given details to the online banking platform or responded to such things, and well, we cannot help that."

As the technological changes of accelerated digitalization also exacerbated fraud practices, consumers were given the responsibility of addressing this increased risk of confidence schemes themselves, which was communicated to them only after they had already changed their banking practices.

Competitive pressures

The experts in the roundtable discussion at the first stage of our research (Fig. 1) were adamant that, had data protection regulations not existed, banks still would have taken special care of their clients' data to maintain trust and signal respect to their clients. However, banking platformization has introduced new actors into the banking network, and the experts noted that these new actors may not recognize the same imperative. They suggested that this has led to a shift in data protection practices.

The roundtable participants expressed concerns that consumers, having become familiar with technology companies such as Apple, Facebook, Google, and Amazon and entrusted these companies with much personal data, would choose convenience over caution regarding the risks of sharing financial data with Big Tech and FinTech as well. The G-SIB's Chief Data Officer mentioned the following in an interview: "If it is only about trust, but your applications are not convenient, I don't think trust will win, unfortunately." Several roundtable participants insisted that banks would cease to exist if they cannot or will not exploit their clients' data in the same manner as their new competitors.

Here, contextual integrity becomes a factor in consumer trust, because the norms in the context of banking differ from those in the context of social media and other Big Tech companies. In a panel discussion on open banking, a representative of a consumer group stated that a higher level of trustworthiness is expected from banks, which have better reputations than Big Tech companies when it comes to protecting personal data.

An internal bank auditor noted the following in an interview: "We as a bank, we really have a lot of data. We know what you earn, we know where you shop […]. We know where you get your fuel for your car. Actually, if we do some basic data analytics on it, we can extract very useful data that we can sell to other companies, based on individual data. Of course it's not allowed due to the legislation that is there. But it's also never something that the bank did, where we could monetize on those data." The strict regulation and reputation sensitivity of banks have caused consumers to become habituated to secure and reliable banking, leaving them untrained to recognize financial and privacy risks in a more open data-sharing environment.

However, banks cannot ignore the competitive pressures of platformization. The head of the data governance department at the G-SIB where we conducted our observations explained that incumbent banks' apps are challenged to compete with FinTech apps with more pleasant interfaces that conveniently combine access to accounts from different banks. He noted that if clients preferred to use FinTech apps that aggregate services, the bank would become the "dumb pipe" in the infrastructure. To prevent becoming obsolete, banking apps need to attain the same ease-of-use and relevance to the client and "be a partner, an app in which you can find lots of stuff." A digital strategist also emphasized the element of "partnership" with clients in his vision for the near-future of banking: "To become a value-added advisor to the customer, instead of racing to the bottom for price, we have to become expert at predicting customer needs and preferences." To this end, client data would need to be used more extensively than banks have done before, and banks would "also need your data from other banks."

Most interviewees refrained from describing FinTech companies as direct competitors, instead depicting them as potential partners in the digital banking "ecosystem." The argument was made that, while FinTechs cannot exist without the infrastructure of banks, banks can exist without FinTechs. In contrast to FinTech start-ups, Big Tech companies were more often depicted as competition, because of their powerful technology and the large amount of personal data they process. The potential of Big Techs to offer more personalized financial services to consumers was seen as the real challenge to the system, because they would have the power to turn banks into "execution-only" infrastructure. As banks would be left with high compliance and maintenance costs of the physical infrastructure, but without more profitable service offerings, this scenario needs to be prevented, in their view.

Some respondents mentioned that something similar had happened in the telecom industry, in which traditional providers have been reduced to maintaining expensive, strictly regulated technological infrastructures, while lightweight Internet-based newcomers have taken off with consumer-facing services. Similarly, FinTech apps can use the secure banking infrastructure to verify identities and make transactions in a black-boxed manner, invisible to clients. Meanwhile, other service providers (e.g., retailers or hospitality providers) can receive transactions through FinTech apps, trusting that the underlying banking system has authenticated clients and verified transactions. In this way, FinTech companies can ride free on the trustworthiness and reliability of the banking infrastructure.

In a panel discussion we organized on sharing bank data with smart cities, experts noted that consumers sometimes hold banks accountable for mishaps that occur on the

end of partners in a data-sharing ecosystem. For example, people may seek recourse from their bank if a third-party provider has a data breach. Consequently, banks are careful about partnerships in such ecosystems. A representative of a supervisory authority mentioned that "it only takes one mistake, one slip-up, or one rogue actor on the market, to perhaps critically undermine the trust of consumers or potential consumers in the entire sector." This again suggests that banks should be careful regarding the contextual integrity of their data-sharing practices.

Measures enacted in response to the COVID-19 pandemic allowed Big Tech and (larger) FinTech companies to further expand their footprint in digital retail financial services, prompting international oversight authorities to issue warnings about incentives for risk-taking by incumbent banks to preserve profitability, particularly in the context of consumer (data) protection risks (FSB 2022). The pandemic shift in social arrangements toward a sharp increase in digitalization has led to the rapid technological remediation of banking practices, with new actors setting new norms for the use of personal data. While incumbent banks may accept these new norms under competitive pressure, the experts interviewed in this study indicated that stretching the contextual integrity of the use of people's financial data has a reputational risk.

Conflicting regulations around data protection

Banks are regulated by a myriad of rules and laws at the national and transnational levels, which entail strict oversight and audit requirements, and banks stand to lose their licenses for non-compliance. A consultant in the European banking sector explained in an interview that regulation "is changing all the time, and becoming more and more severe with the penalties" and internal bank auditors mentioned that "one of the risks that the bank faces is also the non-compliance with the different rules and regulations, and there are more and more," explaining that auditing compliance with "the long list of all the regulations" is increasingly challenging.

The banking representatives in our expert roundtable discussion complained that there is no level playing field when competitors from other sectors enter their market, especially because, from their perspective, enforcement seems to be lax for legislation that is not specific to the financial sector. Banking regulators acknowledge that the risks associated with the complex "black-box" nature of Big Tech platforms' financial activities can be difficult to assess when such companies operate outside established regulatory perimeters (FSB 2022).

A South African consultant had a rather different perspective on the effects of technological mediation on banking and its regulations: "What does it mean to have a level playing field if the game is different? That is in fact what the innovators are doing. They are saying: we are changing the game, not the rules of the game. Changing the whole game, that you might call radical innovation." He argued that "people don't want to bank; they just want a way to transact with money" and "a number of players, including some of the big social media companies and others, will claim that the legislation is inappropriate for the modern ways of doing business."

The roundtable experts also noted that all the different rules that apply to data protection in the banking sector can conflict. For example, Know-Your-Customer (KYC) rules, which are part of transnational Anti-Money Laundering (AML) regulations, require

proof of identification; however, as a roundtable participant remarked, "It is not safe to store an ID card, but you have to show that you are compliant with [KYC] regulations, and this is the proof."

Determining what rules or regulations take precedence in conflict situations is often a complicated matter for banks. In an interview, the Chief Data Officer (CDO) of a major bank explained: "We regularly need to debate what has primacy: our obligation to comply with AML or our obligation to comply with the GDPR. […] It is clear what has primacy, AML, but then you still need to look at the way in which you do that, so you don't carry it out disproportionately." With respect to AML, banks have a gatekeeper function for the financial system. As discussed above, banks are required to conduct KYC verification for the rest of the system to rely on authenticated identities.

The head of an in-house digital legal team specifically pointed to the open banking rules of PSD2 as problematic: "You have the GDPR that has been written by a special division of the European authorities and then PSD2, and they never talked to each other. Just one time somebody maybe thought that it would be interesting to discuss with the GDPR guys and then you have some provision like Article 94[1] of the PSD2. But then, you clearly see that it's totally not aligned." The "GDPR guys" who should have been consulted were working in the office of the European Data Protection Supervisor (EDPS). In our conference panel discussion on data protection and PSD2, one of the "gals" working at that office explained what had gone wrong: "When that legislation was being considered, that obligation to consult with the EDPS had not yet been fully formalized, which maybe partly explains […] that we are now faced with a text with a, let's say, complicated relationship with the GDPR."

One of the main points of contention between PSD2 and the GDPR is the meaning of consent. As the EDPS expert explained: "We have two quite high-profile legal texts, both dealing with consumer data of quite sensitive category, and both use the terms 'consent' and 'explicit consent.' And yet, this all doesn't mean that all those terms mean the same thing. […] Consent in PSD2 is basically a contractual consent, so that means that the individual has to agree to give access in this case to their data, but this is an additional safeguard, this is a 'signing a contract.' […] The consequence of that in the framework of the GDPR is that in many cases under PSD2, the actual legal basis for the processing for personal data would be: contract, or what we call contractual necessity." In practice, this means the GDPR conditions for valid consent (e.g., consent must be specific, informed, and unambiguous; see Fig. 2) do not apply to a situation in which consumers agree to share payment data with a third-party provider. Consequently, it is questionable for financial data-sharing under PSD2 whether (vulnerable) consumers are aware of what exactly they agree to and what the potential risks are.

In response to the pandemic, policy measures were taken worldwide to address the accelerated digitalization of banking, such as higher contactless payment limits and new security standards and guidelines to support a higher reliance on technology, which mainly addressed banks' exposure to cyber risk (FSB 2022). While these policy measures supported the acceleration of digitalization and improved reliability and security, they

[1] Article 94 of PSD2 very summarily covers data protection, highlighting the processing of personal data for fraud detection purposes and referring to compliance with the GDPR (or rather its predecessor, the Data Protection Directive).

did not appear to specifically affect the capabilities of bank staff to protect personal data, although they affect other consumer risks, such as the amount that fraudsters can obtain via instant payments.

Automated creditworthiness assessments

In the "The transparency paradox" section, we refer to the GDPR provisions for transparency in automated decision-making and profiling. Profiling is not uncommon in the financial sector because credit ratings are a mandatory and standard practice. The more available and accurate the data are, the better profiling and credit rating will work. Legally, certain client characteristics, such as gender and ethnicity, are not allowed as factors in these systems; however, there have been data protection cases around profiling systems. For example, the Finnish Data Protection Ombudsman ordered the financial credit company Svea Ekonomi in 2019 to correct its creditworthiness assessment practices, warning that an upper age limit is not acceptable as a factor because age does not describe solvency or willingness to pay.

Explaining automated creditworthiness assessments is considered an important data protection requirement (see Fig. 2). An expert from a central bank, who was involved in discussions of the Basel Committee on Banking Supervision (BCBS) on guidance for AI applications in banking, remarked in an interview: "For a credit decision, you need to be able to explain why you accepted a client or did not accept a client." A data governance expert at the bank where we conducted our observations explained in more detail: "If you are using pure deep learning or even some machine learning that is not very clear, you just don't know why the machine refused somebody. […] For a bank, if it is about refusal of credit, you better have a very clear reason why. Because the clients that are accepted will be happy, [but] the other ones might just leave you and break off the relationship totally and really give you bad advertisement, because it is unfair. And maybe they are right it isn't fair. But if you don't even know why you are refusing them, you cannot react. So those are areas where we will not deploy algorithms which are under the black box model."

A home loan adviser reported sometimes having to explain creditworthiness assessments to clients: "There is not much big data involved yet. Most of the data that I can access or that I need to check, that have been decided by the bank, that is easy to interpret. Sometimes it is a little less clear. But I have to say that at the moment I am not much involved in big data, at the moment I do not really do anything with that." The bank's CDO confirmed that automated creditworthiness assessments mostly happened for business-to-business loans and not yet for consumers, so little personal data are involved currently.

While digitalization increases the amount of data available for creditworthiness assessments, none of the respondents in the second stage of our research discussed accelerated digitalization as an important influence on the personal data protection practices in credit assessments, despite the fact that this was an explicit question in the interviews. Notably, in this respect, most interviews were conducted with representatives of incumbent banks and established financial institutions, and FinTech companies may have different aspirations regarding the use of platform-derived personal data for creditworthiness assessments. Although we recognize this limitation

of our research, we have to conclude that, because the pandemic measures did not appear to have affected this theme in our findings to a noticeable extent, we cannot discuss it here in further detail.

Digital skills and data protection awareness

At several points during our study, it became clear that clients and bank staff did not yet have sufficient digital skills and data protection awareness to cope with the accelerated digitalization brought on by pandemic response measures. The digitalization of services involves more than simply performing the same tasks using digital tools. Practices fundamentally change during the infrastructural change process of platformization. A banking consultant with clients among various European G-SIBs explained that, to properly digitalize a service, "you need to understand the whole process from the contact with the client to the end of the deal, and this requires a completely new set of skills," adding "it's called the transformation not because it's purely a digitalization of the existing [practices]; you have to rethink why you are doing this."

An expert from a central bank stated: "[staff with the right] profiles are rare, and I don't know if traditional banks are a very attractive work environment for people with a data science profile. But in the long term that may be smoothed out and many banks are already working on reskilling their staff. It is also matter of mindsets, changing the culture." Meanwhile, the Belgian CEO of the G-SIB where we conducted our observations noted in an interview with a national newspaper that manual jobs were being automated, and the introduction of robots meant certain jobs would disappear.

Should services be completely digitalized to make in-person contact with bank staff redundant, for instance, when clients request a new loan in-app, specialized expertise would be lost. Translating staff expertise into the design of automated services and optimizing solutions for an app-based service were considered to be complicated. The home loan advisor stated: "You cannot expect everyone to do all those things themselves and know all the details." He explained that processes would need to be simplified for clients with less expertise than bank specialists, and services might consequently become less customizable. The user experience design of a fully digitalized system for non-specialist users must be simpler than the process for specialists. From the perspective of platform studies, the potential effect of process simplification is caused by the different affordances of a fully digital system compared with a system that still incorporates humans.

With regard to employees' data protection awareness, all employees at the G-SIB where we conducted our observations were required to participate annually in a 30-min training webinar on data protection, while some professionals, such as data protection officers, in-house lawyers, the fraud department, and auditors, took more extensive or specialized data protection training. This was confirmed as a standard practice in banks by representatives of other organizations with whom we talked. However, a press officer mentioned: "Those trainings are often 'check the box' exercises. You need to do that, and then you have done it, and you can return to business as usual. But it is exactly business as usual where it happens." Several bank staff members we interviewed recalled having undergone the (one-hour, digital) training but did not remember how long ago it had been. As a problematic example, the press officer also recounted instances in which

account managers sent full portfolios of clients via internal email to colleagues. “It is a continuous education. These things do not happen every week, but it does happen about two, three times a year, and that is two, three times too many.” He added that he had experienced similar problems at other major banks where he had previously worked.

In "The transparency paradox" section, when presenting the findings on transparency and communication, there were also indications that, while the pandemic led to increased (online) communication with clients, staff needed to be trained for such online communication and convey extra warnings and explanations to clients on digital interactions with the bank. Although the pandemic did not cause the digital skills gap, it intersects with accelerated digitalization, bringing to the surface how the human elements in the “old” infrastructure needs to adapt to the remediation of digital technologies to make the system work.

Limitations

This study aimed to explore the effects of accelerated digitalization in retail banking stimulated by the COVID-19 pandemic response measures on the capabilities of European bank staff to protect clients’ personal data. Before discussing our results, we should acknowledge the limitations of our approach that may have affected the generalizability of our findings. Since we sought a nuanced understanding of technological mediation in this context, a qualitative research approach was the most appropriate; however, this approach has some obvious limitations.

Apart from the limited sample of respondents (compared to a large-scale survey), time-limited ethnographic observations necessarily offer no more than a snapshot of a segment of societal development and will yield no information on long-term effects. Although we triangulated our findings with industry documentation and sought validation through the publication of reports and presentations, and explicitly requesting critical feedback, our findings reflect the perspectives of a relatively small sample (25 interviewees and 57 panelists and roundtable participants) of banking and data protection experts. As the findings in the "Automated creditworthiness assessments" section highlight, those experts were predominantly representatives of large banks, which was in line with our focus on the data protection capabilities of bank staff, but nevertheless reflects an underrepresentation of FinTech or Big Tech perspectives. Therefore, our sample is not representative of the full spectrum of the European banking sector in its move toward increased digitalization, platformization, and open finance. These limitations reduce our ability to make generalizations regarding the effects of pandemic response measures on the protection of personal data in retail banking and the related role of bank employees.

Nevertheless, our qualitative approach, including the online panel discussions with (open) banking experts from different countries, regions, and sectors, did provide the rich and nuanced insights we intended to obtain, allowing us to ask for more real-world, “on the ground” details and specifics than surveys or experiments would have afforded. Future research should expand our exploratory analysis to include more diverse sample sizes and seek possible comparisons with other jurisdictions and sectors of the digital economy.

Discussion

Mediation theory predicts that when social arrangements around technology change, people's practices and abilities to communicate also change (Lievrouw 2014). Our findings support this argument. COVID-19 pandemic response measures motivated consumers to adopt platformized digital banking tools at a much higher speed than previously anticipated, which led to increased use of online payment methods, expansion of FinTech businesses, and fast habituation of bank clients to digital banking. In this technological mediation process, communication abilities were reconfigured, practices remediated, and social arrangements reformed. Although it is too early to conclude that these effects of technological mediation will persist, clients who have become habituated to banking apps and online payments are not likely to return to banking at physical branches as their habits will become inextricably connected with on-the-go banking (cf. Orlikowski and Scott 2008).

The analytical framework used in this study, based on mediation theory and combining perspectives from infrastructure and platform studies, contributes to furthering the understanding of the entanglement and important role of bank staff in enabling digital transformation. We found that when digital services, such as banking apps, offer functions previously provided by bank staff, such as customizing financial advice, something may be lost in translation. The client-centered financial expertise of bank staff may not translate well to the simplified user interface of an app. Good customer service "entails matching or adapting the capabilities of a chef to the requirements or desires of the guests," whereas self-service is characterized by "insensitivity to customers" (Scott 2022: 145). Replacing service staff with machines allows banks to standardize and gain control over client options and data (Scott 2022).

In addition, the role of bank staff in mediating payments, which has functioned as an unrecognized impediment to identity fraud, has not yet been translated into platform technology. Instead, the speed and ease of use of platformized banking eradicate the time for consumer reflection on the authenticity of payment requests built into (staffed) banking alternatives with more friction.

Platform technology, while supportive of digital banking, has a program of action ("script") that is aimed at data-sharing, which traditionally is not a common practice in banking (a "remediation of practices," cf. Lievrouw 2014). Banking platformization privileges a social ordering in which clients not only provide money but also personal data to banks. Moreover, while banks focus on the changes in platformized banking to their own and their clients' capabilities, other actors are also recognizing shifts in their capabilities. These include threat actors with an interest in confidence crimes, and non-bank market players who may care more about gathering personal data than providing financial services. Thus, banking platformization changes the context of banking, resulting in a concomitant shift in purposes, values, and functions (cf. Nissenbaum 2010). Information-flow norms in the banking context differ from those for online advertising markets in terms of personal data, and retail banks risk losing clients' trust if they adopt the behavior of "Big Tech" platforms (Aitken et al. 2020).

This trust may be further undermined by the "black-boxing" of digital banking (cf. Latour 1999). Providing intelligible information to clients regarding the usage of personal data in digital banking, including its risks, is essential for both consumer trust and

legal compliance. However, the experts we talked to for this study are doubtful that consumers, especially vulnerable ones, will understand such information. Moreover, banks are reluctant to provide it because (i) it may be commercially sensitive, (ii) banks fear it may annoy clients, and (iii) it could deter clients from sharing data that banks need to remain competitive in the digital environment ("The transparency paradox" section). However, experts see the value of educating clients and presenting banks as safe parties for sharing financial data. Bank staff can play a role in this type of client education.

The idea of banks as safe parties for sharing financial data is undermined by the competitive pressure of Big Tech actors in the digital banking environment. Platformization radically "changes the game" of banking. While the bank experts in our study fear that consumers underestimate the risks of banking through less-regulated digital competitors, banks themselves emulate these competitors' practices by seeking new and more intensive uses for their clients' data, thereby risking the contextual integrity of their use of such data.

The impact of the pandemic has led to a further expansion of Big Tech competitors in digital banking, increasing competitive pressure (FSB 2022). We found it also impacted societal arrangements in banking by abruptly moving all client interactions online (a "reconfiguration of abilities to communicate," cf. Lievrouw 2014), which in itself was received positively by clients, but had the side effect of prompting a steep increase in digital fraud and confidence crimes. Bank clients who had been underinformed beforehand of the risks of digital banking were often unprepared to handle them (Al-Qahtani and Cresci 2022). Thus, actors in confidence crimes have exposed a risk in the digital banking infrastructure: the lack of in-person identity authentication between different platform users, payers, and payees. Those who receive fraudulent payment are also platform users, albeit malicious ones. Bank staff reported feeling powerless to help victimized clients, as clients are considered to have the responsibility of protecting themselves against such risks in the digital banking environment, with platforms being presented as merely neutral infrastructure (Gillespie 2010).

This touches on a technological mediation issue that has become increasingly pressing in recent years: the responsibilities of platform providers (Gillespie et al. 2018). As rule-setters, banking platform providers can be called upon to conduct police activities on their platforms. Banks already perform such tasks in the context of anti-money laundering and terrorist financing enforcement (Ferrari 2020). To prevent confidence schemes, bank platform data can be mined to gain insights into malicious behaviors. The ongoing increase in digital financial fraud and phishing has sparked a societal debate on the responsibilities of financial service providers in educating their clients on the risks of digital banking (UK Parliament 2022); however, this discussion can be taken further in the context of platform governance responsibilities.

Bank staff may have little power to challenge the digitalization of banking, should they want to do so. Our findings are consistent with those of Kitsios et al. (2021), who surveyed Greek bank staff and management and found that many employees fear job cuts but generally welcome the digitalization of banking operations. Technology can be used to undermine workers' power by making it possible to replace them with cheaper labor (Srnicek 2017), such as "robots" or digital assistants. This is in line with Latour (1992),

who argued that technological artifacts privilege certain orderings, sometimes replacing humans entirely ("delegation") by carrying out tasks more efficiently and effectively.

Overall, a recurrent theme in our findings was that bank staff often failed to see the big picture of banking digitalization. We found that short, mandatory online training sessions to raise data protection awareness could be quickly forgotten in daily practice. Instead, a more profound cultural transformation is required. The lack of staff skills to envision an entirely different way of working in the infrastructural change of digital transformation was indicated as a major challenge by several experts. As Mariën et al. (2017) note, strategic skills are often omitted from digital skills training but are in fact highly relevant to digitalization projects. This study serves as a reminder to avoid underestimating the importance of developing both skills and strategic insights among staff in digitalization strategies. In terms of mediation theory, bank staff must be retrained to optimize their role in the new social order and meet the prescriptions of digital banking.

By adopting an encompassing approach to identifying the phenomenon, we found both high-level and on-the-ground effects of the digitalization of banking services on employees' data protection capabilities, from conflicting legislation and competitive pressures to direct communication with clients. The infrastructural change of platformization creates new risks for clients, while digital banking service inscriptions aim to convince consumers to allow for more sharing and reuse of personal data rather than inform them of the risks. Meanwhile, in-person interaction with bank staff, which could play an important role in preventing some risks related to digital fraud, is disappearing as the digitalization of banking progresses.

In brief, the technological mediation of banking platformization is disempowering bank staff in the support they can provide to clients. In the interest of consumer protection, replacing bank staff mediation with technological mediation in banking requires compensatory measures, most notably through public policy interventions such as stricter enforcement of transparency requirements regarding the communication of risks, privacy-by-design and data minimization safeguards to prevent avenues for abuse, and clear responsibilities for platform providers in setting and enforcing consumer-protection rules.

Conclusion

This qualitative research contributes to the academic debate on how digitalization affects everyday practices and the role of humans in this transformation, particularly the role of human work in making the digital work (cf. Ghosh and O'Neill 2020; Harchekar 2018; Mueller 2021). Our analytical framework, which combines mediation theory with the theory of contextual integrity and focuses on infrastructure and platforms, has uncovered nuanced insights into the crucial role of bank staff in helping clients navigate the digital banking environment and develop new habits. Future research on innovation and digitalization may similarly benefit from considering technological mediation and examining how communication abilities are reconfigured, practices remediated, and social arrangements rearranged to obtain a nuanced view of possible tensions between different users and conflicting interests related to innovation.

Our findings show that banking platformization results in a partial displacement of risks from retail banks to their clients and that client-facing employees are disempowered to support clients who struggle to protect themselves from confidence schemes such as identity fraud, phishing, and online scams. In addition, during the pandemic, it became clear that bank staff lacked sufficient digital skills to keep up with accelerated digitalization and strategic insights to adapt to the game-changing impact of infrastructural innovation on their practices. These issues identified in our study could severely hamper public trust in the digital financial service ecosystem.

Our analysis also suggests several practical implications. First, the data protection risks of digital banking *to consumers* need to be elaborated on in more detail and explained to them in clear and easily understandable terms to compensate for the lack of in-person communication with bank staff. Therefore, regulators must focus on enforcing transparency requirements.

Second, new requirements must be introduced for financial service platform providers (including licensed banks) to proactively support people who have been victimized by online fraud. Regulators in the UK are undertaking such measures (Financial Conduct Authority 2022), and other countries and transnational regulators would do well to follow suit.

Third, payment service providers, including banks, should focus their choices on technology development for privacy-by-design and data minimization to prevent the creation of data protection risks, rather than shifting the burden to consumers to protect themselves. Because these are also GDPR requirements, regulators should consider them in their enforcement alongside transparency.

Fourth, more extensive digital skills training for bank staff is needed to achieve a cultural change that fosters more strategic thinking about digitalization and a higher awareness of potential risks to the protection of people's personal data. Training that is more sensitive to the contextual integrity of data processing practices could help sustain trusting relationships with consumers by facilitating greater awareness of contextual norms and the expectations of all stakeholders.

Considering the exploratory nature of this study, further research is needed to improve data protection risk communication in the context of digital banking. Future studies can also focus on comparisons between sectors shaped by digitalization and how social demands shape digital technologies in other contexts.

Abbreviations

AML	Anti-money laundering
API	Application programming interface
BCBS	Basel Committee for Banking Supervision
CDO	Chief data officer
EDPS	European Data Protection Supervisor
FinTech	Financial technology (companies)
GDPR	General Data Protection Regulation
G-SIB	Global Systemically Important Bank
KYC	Know-your-customer
MCS	Media and communication studies
PSD2	The European Union's revised Payments Services Directive
SCOT	Social construction of technology
STS	Science and technology studies
SWIFT	Society for Worldwide Interbank Financial Telecommunications

Supplementary Information

The online version contains supplementary material available at https://doi.org/10.1186/s40854-023-00533-y.

Additional file 1. Interview protocols.

Acknowledgements
The authors thank the editor and anonymous reviewers for their insightful suggestions.

Author contributions
IvZ collected, analyzed and interpreted the data, and wrote the major part of this manuscript. JP has made a substantial contribution to the analysis and interpretation of the data, and read, revised and approved the manuscript.

Funding
This research was conducted within the VUB Chair 'Data Protection On the Ground'. The Chair is coordinated by the research center imec-SMIT (Studies on Media, Innovation & Technology) in collaboration with the research group LSTS (Law, Science Technology & Society), and is financially supported by BNP Paribas Fortis. The latter party has had no role in the design of the study, the analysis, the interpretation of data or in the writing the manuscript, but was supportive in the data collection.

Availability of data and materials
The datasets generated and analysed during the current study are not publicly available due to a non-disclosure agreement between the researchers and the organization(s) at which the study was conducted, as well as confidentiality and protection of anonymity of the respondents (as agreed in the informed consent requests signed by the respondents) but are available from the corresponding author on reasonable request.

Declarations

Competing interests
The authors declare that they have no competing interests

Received: 13 July 2021 Accepted: 19 July 2023
Published online: 20 January 2024

References

Aitken M, Toreini E, Carmichael P, Coopamootoo K, Elliott K, van Moorsel A (2020) Establishing a social licence for financial technology: reflections on the role of the private sector in pursuing ethical data practices. Big Data Soc. https://doi.org/10.1177/2053951720908892

Akrich M (1992) The description of technical objects. In: Shaping technology/building society, studies in socio technical change. MIT Press, Cambridge, pp 205–224

Al-Qahtani AF, Cresci S (2022) The COVID-19 scamdemic: a survey of phishing attacks and their countermeasures during COVID-19. IET Inf Secur 16(5):324–345

App Annie (2020) The impact of coronavirus on the mobile economy. https://www.appannie.com/en/insights/market-data/coronavirus-impact-mobile-economy/. Accessed 11 Jul 2021

Baicu CG, Gârdan IP, Gârdan DA, Epuran G (2020) The impact of COVID-19 on consumer behavior in retail banking. Evidence from Romania. Manag Mark Chall Knowl Soc 15(s1):534–556. https://doi.org/10.2478/mmcks-2020-0031

Benanav A (2020) Automation and the future of work. Verso Books, London

Bennett O (2020) Bank branches: Why are they closing and what is the impact? House of Commons Library. https://researchbriefings.files.parliament.uk/documents/CBP-8740/CBP-8740.pdf. Accessed 11 Jul 2021

Broby D (2021) Financial technology and the future of banking. Financ Innov 7(1):47. https://doi.org/10.1186/s40854-021-00264-y

Brown J, Isaacs D (2005) The world café: shaping our futures through conversations that matter. Berrett-Koehler Publishers, San Francisco

Carbó-Valverde S, Cuadros-Solas PJ, Rodríguez-Fernández F (2022) Entrepreneurial, institutional and financial strategies for FinTech profitability. Financ Innov 8(1):15. https://doi.org/10.1186/s40854-021-00325-2

CB Insights (2018) The challenger bank playbook: how 6 digital banking startups are taking on retail banking. CB Insights: Research Briefs. https://www.cbinsights.com/research/challenger-bank-strategy/. Accessed 11 Jul 2021

Chao X, Kou G, Peng Y, Viedma EH (2021) Large-scale group decision-making with non-cooperative behaviors and heterogeneous preferences: an application in financial inclusion. Eur J Oper Res 288:271–293. https://doi.org/10.1016/j.ejor.2020.05.047

Chen Z, Li Y, Wu Y, Luo J (2017) The transition from traditional banking to mobile internet finance: an organizational innovation perspective—a comparative study of Citibank and ICBC. Financ Innov 3(1):12. https://doi.org/10.1186/s40854-017-0062-0

Citi GPS (2016) Digital disruption—how FinTech is forcing banking to a tipping point. Global Perspectives & Solutions. www.citi.com/citigps. Accessed 11 Jul 2021

Colangelo G, Maggiolino M (2019) From fragile to smart consumers: shifting paradigm for the digital era. Comput Law Secur Rev 35(2):173–181

Couldry N, Hepp A (2013) Conceptualizing mediatization: contexts, traditions, arguments: editorial. Commun Theory 23(3):191–202
Daynes S, Williams T (2018) On ethnography. Wiley
De Goede M (2020) Finance/security infrastructures. Rev Int Polit Econ 28(2):351–368
Denscombe M (2014) The good research guide: for small-scale social research projects. McGraw-Hill Education, London
Dieter M, Tkacz N (2020) The patterning of finance/security: a designerly walkthrough of challenger banking apps. Computational Culture (7). http://computationalculture.net/the-patterning-of-finance-security/
Dörry S, Robinson G, Derudder B (2018) SWIFT as infrastructure intermediary in global financial markets. Financial geography working paper series #22
Dourish P (2004) What we talk about when we talk about context. Pers Ubiquit Comput 8(1):19–30
EBA (2021) Report on the use of digital platforms in the EU banking and payments sector. European Banking Authority. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2021/1019865/EBA%20Digital%20platforms%20report%20-%20210921.pdf. Accessed 28 Feb 2023
Edwards PN, Jackson SJ, Bowker GC, Knobel CP (2007) Understanding infrastructure: dynamics, tensions, and design. http://deepblue.lib.umich.edu/handle/2027.42/49353. Accessed 11 Jul 2021
European Central Bank (2020) Study on the payment attitudes of consumers in the euro area (SPACE). European Central Bank Publications Office, Luxemburg
Exton J (2020) ING survey: we're still suspicious about Open Banking. ING Think. https://think.ing.com/articles/what-we-say-and-what-we-do-differ-in-a-tech-world/. Accessed 6 Oct 2020
Ferrari V (2020) Crosshatching privacy: financial intermediaries' data practices between law enforcement and data economy. Eur Data Prot Law Rev 6(4):522–535
Financial Conduct Authority (2022) Our strategy 2022–2025. https://www.fca.org.uk/publication/corporate/our-strategy-2022-25.pdf. Accessed 28 Feb 2023
Fiserv Annual Payments Research (2020). Payments transformation: immediate, intelligent and inclusive. https://www.finextra.com/finextra-downloads/research/documents/160/payments-transformation-immediate-intelligent-and-inclusive.pdf. Accessed 11 Jul 2021
FSB (2022) FinTech and market structure in the COVID-19 pandemic: implications for financial stability. Financial Stability Board. https://www.fsb.org/wp-content/uploads/P210322.pdf. Accessed 24 Feb 2022
Ghosh I, O'Neill J (2020) The unbearable modernity of mobile money. Comput Support Cooper Work (CSCW) 29(3):227–261. https://doi.org/10.1007/s10606-020-09373-1
Gillespie T (2010) The politics of 'platforms.' New Media Soc 12(3):347–364. https://doi.org/10.1177/1461444809342738
Gillespie T (2018) Regulation of and by platforms. In: Burgess JP, Marwick AE, Poell T (eds) The SAGE handbook of social media. SAGE, London, pp 254–278
Haapio H, Mero J, Karjaluoto H, Shaikh AA (2021) Implications of the COVID-19 pandemic on market orientation in retail banking. J Financ Serv Mark 26(4):205–214. https://doi.org/10.1057/s41264-021-00099-9
Harchekar JS (2018) Digitalization in banking sector. Int J Trend Sci Res Dev (Conference Issue ICDEBI-2018)
Hemachandra S, Sharkasi N (2021) Digital transformation induced by the Covid-19 pandemic. In: Martínez-López FJ, López DL (eds) Advances in digital marketing and eCommerce. Springer, Cham, pp 50–61. https://doi.org/10.1007/978-3-030-76520-0_6
Hendrikse R, Bassens D, van Meeteren M (2018) The Appleization of finance: charting incumbent finance's embrace of FinTech. Finance Soc 4(2):159–180. https://doi.org/10.2218/finsoc.v4i2.2870
Howlett M (2021) Looking at the 'field' through a Zoom lens: methodological reflections on conducting online research during a global pandemic. Qual Res. https://doi.org/10.1177/1468794120985691
Ihde D (1990) Technology and the lifeworld: from garden to Earth. Indiana University Press
Irimia-Diéguez A, Velicia-Martín F, Aguayo-Camacho M (2023) Predicting Fintech innovation adoption: the mediator role of social norms and attitudes. Financ Innov 9(1):36. https://doi.org/10.1186/s40854-022-00434-6
Kitsios F, Giatsidis I, Kamariotou M (2021) Digital transformation and strategy in the banking sector: evaluating the acceptance rate of E-services. J Open Innov Technol Mark Complex. https://doi.org/10.3390/joitmc7030204
Kou G, Olgu Akdeniz Ö, Dinçer H, Yüksel S (2021) Fintech investments in European banks: a hybrid IT2 fuzzy multidimensional decision-making approach. Financ Innov 7:39. https://doi.org/10.1186/s40854-021-00256-y
Latour B (1990) Technology is society made durable. Sociol Rev 38(1_suppl):103–131
Latour B (1992) Where are the missing masses? The sociology of a few mundane artifacts. In: Shaping technology/building society: studies in sociotechnical change, pp 225–228
Latour B (1993) We have never been modern. Harvard University Press, Cambridge
Latour B (1999) On recalling ANT. Sociol Review 47(1_suppl):15–25
Latour B, Woolgar S (1979) Laboratory life. The construction of scientific facts. Princeton University Press, Princeton
Leong E (2020) Open banking: the changing nature of regulating banking data—a case study of Australia and Singapore. Bank Finance Law Rev 35(3):443–469
Li B, Xu Z (2021) Insights into Financial Technology (FinTech): a bibliometric and visual study. Financ Innov 7(1):69
Liébana-Cabanillas F, Muñoz-Leiva F, Molinillo S, Higueras-Castillo E (2022) Do biometric payment systems work during the COVID-19 pandemic? Insights from the Spanish users' viewpoint. Financ Innov 8(1):22. https://doi.org/10.1186/s40854-021-00328-z
Lievrouw LA (2009) New media, mediation, and communication. Inf Commun Soc 12(3):303–325
Lievrouw LA (2014) Materiality and media in communication and technology studies. In: Gillespie T, Boczkowski PJ, Foot KA (eds) Media technologies: essays on communication, materiality, and society. MIT Press, Cambridge, pp 21–51
Löhr K, Weinhardt M, Sieber S (2020) The 'World Café' as a participatory method for collecting qualitative data. Int J Qual Methods 19(01/2020):1–15. https://doi.org/10.1177/1609406920916976
Maiti M, Vuković D, Mukherjee A, Paikarao PD, Yadav JK (2021) Advanced data integration in banking, financial, and insurance software in the age of COVID-19. Softw Pract Exp. https://doi.org/10.1002/spe.3018
Mariën I, Baelden D, Iordache C (2017) Developing digital skills and competences: a quick-scan analysis of 13 digital literacy models. Ital J Sociol Educ 9(02/2017):6–30. https://doi.org/10.14658/pupj-ijse-2017-1-2

Meuser M, Nagel U (2009) The expert interview and changes in knowledge production. In: Bogner A et al (eds) Interviewing experts. Palgrave Macmillan, London, pp 17–42
Mueller G (2021) Breaking things at work: the luddites are right about why you hate your job. Verso Books
Nicholls C (2019) Open banking and the rise of FinTech: innovative finance and functional regulation. Bank Finance Law Rev 35(1):121–151
Nissenbaum H (2004) Privacy as contextual integrity. Wash Law Rev 79(1):119–158
Nissenbaum H (2010) Privacy in context: technology, policy, and the integrity of social life. Stanford University Press
O'Dwyer R (2015) When telcos become banks: sociotechnical control in mobile money. https://sciforum.net/paper/view/2816. Accessed 21 Feb 2023
Orlikowski WJ, Scott SV (2008) 10 Sociomateriality: challenging the separation of technology, work and organization. Acad Manag Ann 2(1):433–474. https://doi.org/10.1080/19416520802211644
Pinch TJ, Bijker WE (1984) The social construction of facts and artefacts: or how the sociology of science and the sociology of technology might benefit each other. Soc Stud Sci 14(3):399–441
Pink S, Horst H, Postill J, Hjorth L, Lewis T, Tacchi J (2015) Digital ethnography: principles and practice. SAGE, Thousand Oaks
Plantin J-C, Lagoze C, Edwards PN, Sandvig C (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. New Media Soc 20(1):293–310. https://doi.org/10.1177/1461444816661553
Remolina N (2019) Open banking: regulatory challenges for a new form of financial intermediation in a data-driven world. SMU working paper 2019/05. Centre for AI & Data Governance
Reynolds F (2017) Open banking: a consumer perspective. Barclays, London
Romānova I, Grima S, Spiteri J, Kudinska M (2018) The payment services directive 2 and competitiveness: the perspective of European Fintech Companies. Eur Res Stud J XXI(2):3–22
Scott B (2022) Cloudmoney: cash, cards, crypto, and the war for our wallets. HarperCollins
Silverstone R (2005) The sociology of mediation and communication. In: Calhoun C, Rojek C, Turner B (eds) The SAGE handbook of sociology. Sage Publications, London, pp 188–207
Srnicek N (2017) Platform capitalism. Polity Press
Swacha-Lech M (2017) The main challenges facing the retail banking industry in the era of digitalisation. Financ Mark 26(4):94–116
UK Parliament (2022) Treasury Committee publishes report on fraud, scams and economic crime. https://committees.parliament.uk/committee/158/treasury-committee/news/160700/treasury-committee-publishes-report-on-fraud-scams-and-economic-crime/. Accessed 2 Feb 2022
Valero S, Climent F, Esteban R (2020) Future banking scenarios. Evolution of digitalisation in Spanish banking. J Bus Account Finance Perspect. https://doi.org/10.35995/jbafp2020013
Van Der Cruijsen C (2020) Payments data: do consumers want banks to keep them in a safe or turn them into gold? Appl Econ 52(6):609–622. https://doi.org/10.1080/00036846.2019.1659493
Van Zeeland I, Pierson J (2021) How standards co-shape personal data protection in the European banking sector. In: 2021 IEEE European symposium on security and privacy workshops (EuroS&PW), pp 359–366
Verbeek P-P (2005) What things do: philosophical reflections on technology, agency, and design. The Pennsylvania State University Press, Universiy Park
Verbeek P-P (2015) Beyond interaction: a short introduction to mediation theory. ACM Interact 22(3):26–31. https://doi.org/10.1145/2751314
Westermeier C (2020) Money is data—the platformization of financial transactions. Inf Commun Soc 23(14):2047–2063. https://doi.org/10.1080/1369118X.2020.1770833
Which? Money (2023) Bank branch closures: Is your local bank closing? Which? https://www.which.co.uk/money/banking/switching-your-bank/bank-branch-closures-is-your-local-bank-closing-ayYyu4i9RdHy#headline_1. Accessed 22 Feb 2023
Winner L (1980) Do artifacts have politics? In: Computer ethics, pp 122–192
Wisniewski TP, Polasik M, Kotkowski R, Moro A (2021) Switching from cash to cashless payments during the COVID-19 pandemic and beyond. SSRN Electron J. https://doi.org/10.2139/ssrn.3794790
Yao Y, Li J (2022) Operational risk assessment of third-party payment platforms: a case study of China. Financ Innov 8(1):19. https://doi.org/10.1186/s40854-022-00332-x

Publisher's Note