Routledge
Taylor & Francis Group

Journal of Information Technology Case and Application Research

ISSN: 1522-8053 (Print) 2333-6897 (Online) Journal homepage: www.tandfonline.com/journals/utca20

Digital responsibility as responsible organizing

Nikolaus Obwegeser, Marie Peškova, Margeret Hall & George Grispos

To cite this article: Nikolaus Obwegeser, Marie Peškova, Margeret Hall & George Grispos (22 Jan 2026): Digital responsibility as responsible organizing, Journal of Information Technology Case and Application Research, DOI: 10.1080/15228053.2026.2614300

To link to this article: https://doi.org/10.1080/15228053.2026.2614300

Published online: 22 Jan 2026.

JOURNAL OF INFORMATION TECHNOLOGY CASE AND APPLICATION RESEARCH
https://doi.org/10.1080/15228053.2026.2614300

Digital responsibility as responsible organizing

Nikolaus Obwegeser[a], Marie Peškova[a], Margeret Hall[b], and George Grispos[b]

[a]Bern University of Applied Sciences, Bern, Switzerland; [b]University of Nebraska at Omaha, Omaha, USA

ABSTRACT

Digital responsibility has become a managerial and societal imperative as digital technologies increasingly function as infrastructures of decision-making that shape access to work, welfare, information, and safety. Although ethical principles for digitalization have largely converged, many organizations struggle to translate values into operational routines, allocate accountability, and learn from emergent harms. Consequently, we argue that digital responsibility is best studied and enacted as responsible organizing, i.e. the (inter-)organizational capability to govern digital systems across their lifecycle in ways that are auditable, contestable, and adaptive. This article develops three distinct arguments to support this direction. First, responsibility becomes consequential only when embedded in situated governance through roles, decision rights, artifacts, and escalation routines. Second, accountability is distributed across supply chains and platforms, requiring boundary-spanning governance mechanisms that can travel across organizational interfaces. Third, responsibility depends on measurement and learning loops that connect ethical intent to observed outcomes.

Introduction

Digital responsibility has moved from an aspirational discourse to an operational demand. Organizations now deploy systems that do not merely support decision-making but often constitute it: they recommend who receives credit, shape what information people encounter, allocate work in platforms, and automate eligibility determinations in public administration (Shrestha et al., 2019). These systems scale quickly, act consistently, and connect across organizational boundaries (Obwegeser et al., 2020); yet they also introduce ethical risks that are difficult to anticipate and contest, including opacity, uneven error burdens, and the concentration of power in infrastructures and intermediaries. The idea of digital responsibility (DR) has thus emerged to capture the normative expectations that govern how organizations design and use digital technologies and data (Lobschat et al., 2021; Trier et al., 2023). In organizational contexts, DR is often expressed as corporate digital responsibility (CDR): the firm-level commitment to align digital innovation with societal values such as privacy, fairness, transparency, and sustainability (Lobschat et al., 2021). Yet the proliferation of corporate commitments has not eliminated practical failures. A key diagnosis in the ethics and IS literatures is that principles alone do not guarantee ethical outcomes because they frequently fail at the point of implementation: where design choices, data decisions, procurement arrangements, and operational routines actually determine impacts (Jobin et al., 2019; Mittelstadt, 2019).

This article therefore argues for a paradigm shift in the academic discourse to make the DR implementation problem analytically tractable and practically actionable: digital responsibility is best understood as responsible organizing. By responsible organizing, we mean the capability – within and across organizations – to translate values into lifecycle governance that is auditable, contestable, and adaptive. Auditability signals that DR must be demonstrable rather than merely asserted; contestability signals that affected stakeholders require possibilities for explanation, challenge, and remedy; adaptability signals that responsible conduct must persist even when drift, updates, and changing use contexts alter the technology over time. A key supporting driver for this discourse shift is based on the practical observation that many digital ethics failures are not caused by ignorance of principles, but by weaknesses in organizing, including unclear

CONTACT Nikolaus Obwegeser nikolaus.obwegeser@bfh.ch Institute for Digital Technology Management, Bern University of Applied Sciences, Brückenstrasse 73, Bern 3005, Switzerland

decision rights, incentives that prioritize speed over scrutiny, boundary conflicts in ecosystems, and insufficient monitoring after deployment.

In the remainder of this article, we present three interlocking arguments for a focus on responsible organizing. First, responsibility becomes consequential only when embedded in situated governance through roles, decision rights, artifacts, and escalation routines that shape everyday development and use. Second, responsibility is increasingly distributed across digital ecosystems, which demands governance mechanisms that travel across organizational interfaces rather than relying on firm-centric control. Third, responsibility must be sustained through measurement and learning loops that connect ethical intent to outcomes and enable redress, without reducing ethics to simplistic metrics.

From principle convergence to implementation gaps

A striking feature of the contemporary ethics landscape is the extent of agreement at the level of principles. Comparative analyses of global AI ethics guidelines identify recurring commitments to transparency, fairness, accountability, privacy, and beneficence (Jobin et al., 2019). This convergence has enabled organizations to adopt ethics charters and codes, and it has stimulated the creation of governance toolkits and standards. Yet a recurrent critique is that the same convergence can conceal unresolved questions: which transparency is meaningful in which setting; which fairness definition is appropriate; how responsibility is allocated when harms arise; and how trade-offs are justified when values conflict (Elliott & Copilah-Ali, 2024; Mittelstadt, 2019). This implementation gap has several sources. First, ethical language is often decoupled from technical and managerial decision points (Carl et al., 2023). Teams may endorse fairness while lacking access to relevant demographic data, uncertainty estimates, or stakeholder feedback. Second, organizational incentives often reward rapid deployment, feature delivery, and growth, while ethical review is treated as a frictional afterthought (Taddeo & Floridi, 2025). Third, in ecosystems, the locus of decision-making is fragmented: vendors provide models; integrators assemble systems; platforms set rules; deployers operate services; and affected stakeholders are distant from design choices (Stahl, 2022). This fragmentation encourages responsibility handoffs, in which each actor acknowledges ethical principles while positioning accountability elsewhere.

A productive way to conceptualize this gap is as the accumulation of ethical debt, similar to technical debt (Hron et al., 2022): deferred moral and governance decisions become embedded in systems and later reappear as conflicts, harms, and costly redesign. Operationalizing responsibility is therefore not simply a matter of adding ethics statements; it is a matter of building organizational capabilities that make ethical trade-offs visible, reviewable, and revisable over time. In the following, we present each argument in detail, illustrate practical examples, and discuss implications for IS research.

Argument 1: situated governance makes responsibility consequential

The first argument is that DR becomes consequential only when embedded in situated governance. In other words, responsibility is enacted in specific work contexts – product teams, procurement units, compliance functions, and frontline operations – rather than at the abstract level of principles. Responsibility therefore depends on practical mechanisms: who has the authority to delay or stop deployment; what documentation is required; which risks must be evaluated; how exceptions are handled, and how decisions are recorded for later scrutiny.

A useful positive example comes from efforts to institutionalize digital ethics through governance bodies and risk assessment routines. Nemat et al. (2023) describe the "Principle-at-Risk Analysis" (PaRA) as a standardized tool developed to help interdisciplinary ethics panels translate abstract principles into operational risk assessment in concrete initiatives. The importance of such approaches lies not in any single instrument, but in the institutionalization of responsibility as repeatable practice and shared language for surfacing value conflicts, documenting mitigations, and creating escalation paths. As part of this special issue, Lucas et al. (2025) further develop this framework into a generative AI ethics framework to foster active engagement and responsible innovation. The significance of situated governance is also revealed by failure cases where automation was introduced without adequate contestability and accountability. The Australian "Robodebt" scheme illustrates how scaled decision infrastructures can generate systemic harm

when governance fails to provide effective review, correction, and redress (Nikidehaghani et al., 2023). This governance lesson is not limited to the public sector. In any domain, if decision authority becomes aligned with system outputs while mechanisms for challenge and correction remain weak, responsibility becomes largely symbolic.

A common counterpoint is that governance-heavy approaches slow innovation and advantage incumbents with large compliance capacities (Aghion et al., 2023). This concern warrants a qualifier: responsible organizing should be risk-proportionate. Not every digital initiative requires the same depth of review, and governance should be designed to scale with harm potential, scope, and irreversibility (Obwegeser et al., 2020). At the same time, the speed versus responsibility trade-off is often overstated and depends on the boundary of the system under observation. Weak governance can appear fast in the short term while producing slowdowns later through reputational crises, legal exposure, and costly rework. In this sense, situated governance can even be understood as an enabling capability that stabilizes innovation by reducing the likelihood of catastrophic breakdown.

For IS research, the situated-governance argument directs attention to mechanisms rather than slogans. Empirically, the central questions are how governance is designed, how it is enacted under time pressure, and how it interacts with organizational incentives. Theoretically, these questions connect to long-standing IS concerns, including for example the entanglement of social and material agency (Leonardi, 2011), the role of routines and infrastructures in shaping action, and the governance of IT as a socio-technical system rather than a purely technical artifact.

Argument 2: ecosystem accountability requires boundary-spanning governance

As digital responsibility is increasingly distributed across ecosystems, firm-centric governance is insufficient (Hall et al., 2025). Digital systems are assembled from layered dependencies – cloud platforms, third-party data, open-source components, and, increasingly, general-purpose AI models (Wirtz et al., 2023). In such settings, the actor deploying a system may not control the assumptions embedded upstream (training data, model objectives, update policies), while the actor providing a component may not control downstream use contexts (task framing, stakeholder impacts, operational constraints). Responsibility must therefore be organized across interfaces (Stahl, 2024).

The UK Post Office Horizon case illustrates how responsibility failures can persist when accountability is fragmented and contestation is difficult (Mason, 2021). The statutory inquiry's remit explicitly includes gathering evidence from affected persons, Post Office Ltd, government bodies, Fujitsu, and others, and considering lessons and cultural change – an acknowledgment that failure cannot be reduced to a single technical defect or a single organizational actor. The broader point is that when information systems become infrastructures of organizational authority, contestability becomes a central ethical and governance requirement (Hall et al., 2025). If affected parties cannot access meaningful explanations and if institutional authority treats system outputs as presumptively correct, the system can become an instrument of injustice rather than an aid to accountability. Contemporary developments in algorithmic management provide a second illustration of ecosystem accountability pressures. Workers and advocacy groups have pursued legal and regulatory strategies to obtain transparency about algorithms that allocate work or set pay, highlighting that responsibility claims are frequently contested at the boundaries between platform rules, data practices, and labor conditions. For example, reporting has described legal demands and disputes concerning AI-driven pay systems and transparency for gig-economy workers in Europe (Affolter et al., 2025). While the empirical details of such disputes vary, they underscore a structural feature: in platforms, governance is often exercised through code and terms of service rather than through negotiated organizational processes. This intensifies the need for negotiated, boundary-spanning responsibility mechanisms. Policy developments reinforce the same direction. The European Commission's announcement that the AI Act entered into force in 2024, with phased application including provisions for general-purpose AI, signals a regulatory move toward lifecycle and supply-chain accountability rather than reliance on voluntary principles.

Whether one views regulation as adequate or not, it reflects an institutional expectation that ecosystem actors can document system characteristics, manage risk categories, and clarify obligations across roles such as provider, deployer, and importer. The implication is that responsible organizing must create traveling

governance mechanisms that cross organizational boundaries: documentation expectations, audit rights, incident disclosure norms, and provenance practices that make dependencies legible. The goal is not to dissolve accountability into diffusion, but to specify responsibilities at interfaces so that responsibility becomes operational rather than rhetorical.

This argument suggests a research shift from firm-level programs to ecosystem arrangements (Stahl, 2024). Studying responsibility handoffs – how accountability is negotiated in procurement contracts, platform policies, model documentation, and incident reporting – requires interorganizational case designs and process tracing. It also invites tighter integration between platform studies, digital infrastructure research, and governance scholarship.

Argument 3: learning loops sustain responsibility over time

The third argument is that responsible organizing requires measurement and learning loops. Digital systems drift, data distributions change, user behaviors evolve, adversaries adapt, and organizational incentives change (Pentland et al., 2020). A one-time ethical review cannot sustain responsibility when systems are updated continuously or re-purposed across contexts. Responsibility must therefore be organized as ongoing learning: monitoring, incident response, post-incident analysis, and governance adaptation.

Here, a tension must be addressed directly. Measurement is necessary for learning, yet responsibility cannot be reduced to simplistic metrics. Ethical qualities such as dignity and autonomy resist quantification, and metric regimes can produce perverse incentives (Leidner & Tona, 2021). Responsible organizing therefore requires a portfolio approach: combining quantitative indicators (e.g., subgroup error patterns, complaint volumes, audit findings) with qualitative review (case-based audits, stakeholder engagement, red-team exercises) and procedural safeguards (appeals mechanisms, documentation that enables scrutiny). Measurement, in this view, supports governance decisions – pause, redesign, constrain use, invest in mitigation – rather than substituting for ethical judgment. Real-world generative AI incidents illustrate why learning loops are now indispensable. In June 2023, a U.S. judge sanctioned lawyers who submitted a brief containing fictitious case citations generated by ChatGPT – an anecdote that is widely cited as a cautionary example of hallucination risk and the failure of verification routines (Milmo, 2023). The core responsibility issue here is not simply that a model can produce false outputs but that organizations and professionals must organize verification, accountability, and escalation practices appropriate to probabilistic systems. Learning loops – monitoring failure modes, updating policies, improving training and workflow design – become a central component of responsible use.

For IS scholarship, the learning-loop argument raises questions about the micro-foundations of responsibility over time: how organizations detect harms early; how they attribute causality across socio-technical systems; how they decide when to roll back or restrict systems; and how they institutionalize lessons so that ethical debt does not recur. It also strengthens the case for design-oriented research that creates and evaluates artifacts enabling monitoring, contestability, and auditable learning (Gregor & Hevner, 2013).

Turning defensive compliance into trustworthy innovation

Many organizations have responded to DR with toolkits, checklists, and governance frameworks. These instruments, as described in articles that are part of this special issue (e.g., Lucas et al., 2025) are valuable, insofar as they function as boundary objects – shared templates and routines that carry ethical considerations into design and deployment. Yet they can also become symbolic if adopted primarily for reputational or compliance reasons. The risk is ethics washing: visible commitment without operational transformation. Mittelstadt's (2019) critique that principles alone cannot guarantee ethical AI generalizes here: tool adoption without changes in authority, incentives, and learning capacity may create the appearance of responsibility while leaving the socio-technical production of harm intact. A more robust framing treats digital responsibility as an organizational capability that can support trustworthy innovation. When organizations systematically embed governance, interface accountability, and learning loops, they reduce the likelihood of catastrophic failure and increase the plausibility of legitimate digital transformation. This framing aligns with CDR research that emphasizes responsibilities toward stakeholders and society (Lobschat et al., 2021) and with IS work that places dignity and human values at the center of digitalization (Leidner & Tona, 2021). The crucial point is that responsibility is not merely an external

constraint; in digital economies characterized by opacity and asymmetry, trustworthy conduct can become a strategic asset – though only if it is backed by demonstrable practices rather than marketing claims.

Conclusion and implications

Digital responsibility is frequently treated as a matter of principles, pledges, and compliance. This article shows that such treatments remain inadequate unless responsibility is enacted as responsible organizing: auditable, contestable, and adaptive governance embedded in lifecycle practices and extended across ecosystems.

Treating DR as responsible organizing clarifies what should be studied and designed. First, research should examine situated governance in action: how decision rights are allocated; how teams interpret and operationalize value commitments; how ethics reviews function under time pressure; and how escalation and redress mechanisms operate when harms are alleged. Second, research should follow responsibility across ecosystems. Interorganizational case research and mixed-method designs can illuminate how procurement contracts, platform policies, model documentation, and regulatory obligations distribute responsibility; how accountability is displaced through boundary work; and how affected stakeholders gain or lose contestability. Third, research should foreground temporality. Responsibility is not an event; it is a trajectory. Longitudinal studies can show how organizations adapt governance over time, how learning from incidents becomes institutionalized (or fails), and how ethical debt accumulates in digital infrastructures. Finally, responsible organizing invites multi-level theorizing. Individual moral agency, organizational governance, institutional regulation, and societal power relations intersect in the operation of digital systems.

In practical terms, the core challenge is not a lack of ethical vocabulary, but the organization of accountability in socio-technical systems that scale and interconnect. In scholarly terms, the opportunity for IS research is to develop empirically grounded explanations and designable mechanisms that help organizations govern digital technologies toward legitimate and humane outcomes.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Nikolaus Obwegeser is a Professor of Information Systems and head of the Institute for Digital Technology Management at the Business School of the Bern University of Applied Sciences (BFH), Switzerland. His current work focuses on digital business transformation and digital innovation, with additional interests in agile methods and tools, information systems development, and corporate digital responsibility. Prior to joining BFH, he served as Associate Director at IMD's Global Center for Digital Business Transformation in Lausanne and held a faculty position at Aarhus University. He earned his PhD from the Vienna University of Economics and Business. Nikolaus currently leads several large EU projects on the intersection between digital technology and societal challenges. He publishes his insights in both scholarly and practitioner outlets and regularly advises both private and public organizations in the area of responsible digital transformation.

Marie Peškova is a Professor at the Institute for Digital Technology Management, Business School, Bern University of Applied Sciences. Her work centres on Corporate Digital Responsibility (CDR) and the "twin transition" at the intersection of digitalisation and sustainability. She teaches Digital Responsibility and integrates CDR perspectives across BFH's postgraduate and executive education portfolio, including the MAS in Sustainable Transformation and the EMBA Project Management programme, and she initiated and co-leads the CAS Digital Responsibility & Risk. As a researcher at the BFH Digital Responsibility Lab, she contributes to CDR research projects such as DIRECT (DIgital Responsibility EduCation and Training), an EU-funded initiative developing a Digital Responsibility competence framework and scalable learning pathways including a learning platform for systematic upskilling. She holds a PhD in economics (University of Fribourg) and completed executive education in Digital Business at MIT Sloan.

Margeret Hall is an Associate Professor of Information Systems and Quantitative Analysis at the University of Nebraska at Omaha (UNO). A social scientist by training, her research focuses on socio-technical systems, AI applications, and technical education. She currently serves as UNO's Faculty Fellow in Artificial Intelligence, and she completed her doctoral and postdoctoral work at the Karlsruhe Institute of Technology. Dr. Hall has been awarded competitive funding from National Science Foundation, the US Department of Energy, and Facebook Research among others, with works appearing in top journals including Renewable and Sustainable Energy Reviews and Artificial

Intelligence Review and conferences including ACM Human Factors in Computing Systems and AIS International Conference on Information Systems. Her NSF-funded work on designing and delivering enterprise computing education for marginalized adult learners was awarded the 2025 Tech Community Engagement Award by the Aksarban Foundation.

George Grispos is currently an Associate Professor of Cybersecurity at the University of Nebraska at Omaha (UNO). He received his PhD in Computing Science from the University of Glasgow in the United Kingdom, where his thesis examined the quality of data in cyber investigations. Prior to joining UNO, Dr. Grispos was a Postdoctoral Researcher with Lero, the Research Ireland Centre for Software in Limerick, Ireland. As of January 2026, he has published fifty peer-reviewed publications related to cybersecurity and digital forensics. On Google Scholar, his citation count is 1,398, with an H-index of 21 and an i10-index of 30. He has received just over four million dollars in funding from various mechanisms including the National Science Foundation, the Department of Justice, and the Department of Homeland Security. His research interests include cybersecurity, digital forensics, critical infrastructure settings, and cybercrime.

References

Affolter, L., Spurk, D., & Straub, C. (2025). Living a calling despite the challenges of the gig economy? The role of meaning-making and work alienation. *Journal of Vocational Behavior*, *162*, 104175. https://doi.org/10.1016/j.jvb.2025.104175

Aghion, P., Bergeaud, A., & Van Reenen, J. (2023). The impact of regulation on innovation. *American Economic Review*, *113*(11), 2894–2936. https://doi.org/10.1257/aer.20210107

Carl, K. V., Kubach, M., & Mihale-Wilson, C. (2023, September). The motivation of companies to implement corporate digital responsibility activities voluntarily: An empirical assessment. International Conference on Wirtschaftsinformatik (pp. 39–52). Springer Nature Switzerland, Cham.

Elliott, K., & Copilah-Ali, J. (2024). Implementing corporate digital responsibility (CDR): Tackling wicked problems for the digital era: Pilot study insights. *Organizational Dynamics*, *53*(2), 101040. https://doi.org/10.1016/j.orgdyn.2024.101040

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, *37*(2), 337–355. https://doi.org/10.25300/MISQ/2013/37.2.01

Hall, M., Pavlakis, A., & Friend, M. (2025). Who counts? A compassionate critique of stakeholder theory in information systems. *Communications of the Association for Information Systems*, *57*(1), 672–682. https://doi.org/10.17705/1CAIS.05729

Hron, M., Obwegeser, N., & Müller, S. D. (2022). Innovation drift: The influence of digital artefacts on organizing for innovation. *Innovation*, *24*(1), 168–200. https://doi.org/10.1080/14479338.2021.1937185

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389–399. https://doi.org/10.1038/s42256-019-0088-2

Leidner, D. E., & Tona, O. (2021). The care theory of dignity amid personal data digitalization. *MIS Quarterly*, *45*(1), 343–370. https://doi.org/10.25300/MISQ/2021/15941

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly*, *35*(1), 147–167. https://doi.org/10.2307/23043493

Lobschat, L., Mueller, B., Eggers, F., Brandimarte, L., Diefenbach, S., Kroschke, M., & Wirtz, J. (2021). Corporate digital responsibility. *Journal of Business Research*, *122*, 875–888. https://doi.org/10.1016/j.jbusres.2019.10.006

Lucas, S., Heinitz, R. M., Becker, S. J., & Charton, J. E. (2025). Developing a framework for addressing ethical challenges in generative AI. *Journal of Information Technology Case and Application Research*, 1–15. https://doi.org/10.1080/15228053.2025.2558443

Mason, S. (2021). The post office horizon scandal: A brief chronology. *Digital Evidence and Electronic Signature Law Review*, *18*, 1–9. https://journals.sas.ac.uk/deeslr/article/view/5390/5188

Milmo, D. (2023). Two US lawyers fined for submitting fake court citations from ChatGPT. The Guardian. Retrieved December 12, 2025, from https://www.theguardian.com/technology/2023/jun/23/two-us-lawyers-fined-submitting-fake-court-citations-chatgpt

Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI. *Nature Machine Intelligence*, *1*(11), 501–507. https://doi.org/10.1038/s42256-019-0114-4

Nemat, A. T., Becker, S. J., Lucas, S., Thomas, S., Gadea, I., & Charton, J. E. (2023). The principle-at-risk analysis (PaRA): Operationalising digital ethics by bridging principles and operations of a digital ethics advisory panel. *Minds and Machines*, *33*(4), 737–760. https://doi.org/10.1007/s11023-023-09654-w

Nikidehaghani, M., Andrew, J., & Cortese, C. (2023). Algorithmic accountability: Robodebt and the making of welfare cheats. *Accounting, Auditing & Accountability Journal*, *36*(2), 677–711. https://doi.org/10.1108/AAAJ-02-2022-5666

Obwegeser, N., Yokoi, T., Wade, M., & Voskes, T. (2020). 7 key principles to govern digital initiatives. *MIT Sloan Management Review*, *61*(3), 1–9.

Pentland, B. T., Liu, P., Kremser, W., & Hærem, T. (2020). The dynamics of drift in digitized processes. *MIS Quarterly*, *44*(1), 19–48. https://doi.org/10.25300/MISQ/2020/14458

Shrestha, Y. R., Ben-Menahem, S. M., & Von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review*, *61*(4), 66–83. https://doi.org/10.1177/0008125619862257

Stahl, B. C. (2022). From computer ethics and the ethics of AI towards an ethics of digital ecosystems. *AI and Ethics*, *2*(1), 65–77. https://doi.org/10.1007/s43681-021-00080-1

Stahl, B. C. (2024). From corporate digital responsibility to responsible digital ecosystems. *Sustainability*, *16*(12), 4972. https://doi.org/10.3390/su16124972

Taddeo, M., & Floridi, L. (Eds.). (2025). Digital ethics. *A Companion to Digital Ethics*, 1–9. John Wiley & Sons. https://onlinelibrary.wiley.com/doi/book/10.1002/9781394240821?msockid=11eb56cb9cd766f61ae843039ddc6712

Trier, M., Kundisch, D., Beverungen, D., Müller, O., Schryen, G., Mirbabaie, M., & Trang, S. (2023). Digital responsibility: A multilevel framework for responsible digitalization. *Business & Information Systems Engineering*, *65*(4), 463–474. https://doi.org/10.1007/s12599-023-00822-x

Wirtz, J., Kunz, W. H., Hartley, N., & Tarbit, J. (2023). Corporate digital responsibility in service firms and their ecosystems. *Journal of Service Research*, *26*(2), 173–190. https://doi.org/10.1177/10946705221130467