FILOZOFIA
Volume 80, Number 3, 2025

DOI: https://doi.org/10.31577/filozofia.2025.80.3.3

Data Toxicality: A Techno-Philosophical Inquiry into Digital Harm

GERHARD SCHREIBER, Faculty of Humanities and Social Sciences, Helmut Schmidt University/University of the Federal Armed Forces Hamburg, Germany

SCHREIBER, G.: Data Toxicality: A Techno-Philosophical Inquiry into Digital Harm
FILOZOFIA, 80, 2025, No 3, pp. 300 – 313

In biochemistry, toxicity denotes the potential of a substance to cause harm within a biological system. Over time, the concept has been extended beyond its scientific origins to describe forms of social and psychological harm, as reflected in expressions like "toxic masculinity" or "toxic relationships." This paper introduces the concept of "data toxicality," a techno-philosophical perspective on harmful socio-psychological effects emerging from data practices in the digital age. Unlike biochemical toxicity, data toxicality manifests in interpersonal and institutional dynamics, affecting autonomy, power structures, and digital ethics. The discussion examines both direct and indirect harms resulting from data misuse, surveillance, and algorithmic bias, while considering "unfindability" as a conceptual alternative to data deletion.

Keywords: data toxicality – techno-philosophy – digital ethics – digital harm – surveillance and autonomy – unfindability – structural violence

Introduction

In the biochemical context, the term "toxic"[1] refers to harmful effects a substance can exert on a biological system, such as those of humans, animals, or plants. Extending this scientific usage, "toxic" and "toxicity" have increasingly been applied to socially destructive patterns of thought and behavior that metaphorically "poison" communal or societal interactions (e.g., "toxic masculinity"). Over time, the concept has been further generalized to

[1] The adjective derives from the Greek *toxikón* (τοξικόν), meaning "poison used to coat arrowheads," or simply "arrow poison"; from *toxikós* (τοξικός), meaning "pertaining to bows and arrows" (Passow 1825, 876; translation mine).

describe phenomena associated with risk and/or dysfunctionality, leading to negative outcomes, such as "toxic financial assets," "toxic relationships," "toxic work environments," and even compulsively optimistic "toxic positivity."

In this sense, the concept of "data toxicality," introduced in this paper,[2] builds on and refines the expansion of the meaning of "toxicity." Using the terms "toxical" and "toxicality"[3] instead of "toxic" and "toxicity" foregrounds the socio-psychological dimension of harmful effects – specifically those that manifest in interpersonal relationships and social interactions. Beyond the toxic effects observed in the pharmacological, biochemical, genetic, physical, or physiological domains, the notion of "data toxicality" seeks to conceptualize the potential harms that data can inflict upon human coexistence.

Before presenting selected examples of data toxicality and engaging in techno-philosophical as well as digital-ethical reflections on how to address such harmful effects, the notion of harm in this context must first be clarified.

I. Harm and Its Conceptual Boundaries

Harm encompasses both the process of being harmed and the state of having been harmed, wherein the inflicted or suffered "damage" comprises "a negative, impairing impact and what it entails in terms of loss, destruction, or disadvantage" (Pfeifer 1989, 1486; translation mine). Therefore, harm refers not only to the harmful act itself, but also to the broad spectrum of immediate or indirect consequences that may follow. However, defining any negative impact as harm would result in an overly abstract concept, thereby rendering it impractical. Therefore, in line with Paracelsus's famous maxim, it must be stated: *dosis facit venenum* – the dose makes the poison.[4]

Harm occurs only when a normatively defined threshold – legally speaking, a threshold of significance – is met or exceeded. This is undoubtedly the case with inflicted physical or psychological injuries, as well as violations of individual rights to freedom and self-determination, which, when imposed through external coercion, may also be classified as acts of violence (Schreiber 2022a, 84 – 86). Strictly speaking, a harmful effect presupposes agency, which

[2] While the core concept was first developed in an earlier German-language essay (Schreiber 2022b), this article provides a significantly reworked and updated version, adapted for an international academic readership.

[3] On this neologism, see Gennermann (2020).

[4] However, in the original *Septem Defensiones* (1537/1538), Paracelsus phrased it conversely: "All things are poison, and nothing is without poison; only the dose makes a thing not a poison" (Paracelsus 1928, 138; translation mine).

can be understood both personally and impersonally, i.e., in a subject-analogous manner, and can thus be attributed to specific individuals as well as structures and conditions (Schreiber 2024).

As a specific form of impact, harm is necessarily relational: it always manifests in relation to something or someone, though this does not mean that it is always perceived as such by those affected. As all harm is relational, it does not exist in isolation. This does not suggest that harm always involves a concretely identifiable subject acting against an equally identifiable object; rather, it asserts that harm does not occur unless it affects something or someone in some way. This reveals the passive dimension of harm – *passive* in accordance with the primary meaning of the Greek πάσχειν as the experience of an external influence (Passow 1825, 399), initially without any negative or positive valuation, thus separating the identification of an influence from its evaluation.

The intrinsic relationality of harm corresponds to the fact that the toxic effect of a substance in the biochemical domain presupposes its contact with a living organism – its harmful effect, whether immediate (acute) or gradual (chronic), only manifests when an organism is exposed to it and absorbs it in some manner (e.g., orally, dermally, or through inhalation). Similarly, it can be said that data is not inherently harmful but rather becomes so through its effects on something or someone. This comparison justifies likening data to hazardous materials such as asbestos (Véliz 2021, 107), a chemically benign fibrous silicate with excellent technical properties, whose potentially devastating harmful effects only arise through exposure to its fibers.

II. Concrete Examples of Data Toxicality

Due to the variety of ways in which data can be generated, transferred, analyzed and utilized, we are faced with a correspondingly complex and multifaceted field of phenomena. Thoroughly exploring this domain necessitates a multi-perspective approach that is sufficiently nuanced to capture the distinctions between individual phenomena, yet cohesive enough to avoid artificial fragmentation. Provisionally, one might distinguish between phenomena in which data – despite the common assumption that it is merely "used" or exists "for use," implying utility as the primary characteristic – exerts a directly harmful effect and those in which the harm is indirect. In the former case, harm is explicitly intended and deliberately inflicted, whereas in the latter, harm occurs incidentally and may be tacitly accepted as an unintended consequence. The first category encompasses cases where data is intentionally used by identifiable actors to harm equally identifiable counterparts, making the harm more visible. By contrast, the second category – as explored below in Section B – concerns more diffuse forms of harm that manifest at the collective or societal level. In such instances, neither a distinct perpetrator nor a clear causal link between agent and affected party is readily identifiable.

However, this distinction should not be seen as mutually exclusive. On the contrary, the field is marked by fluid boundaries and inherent ambiguity. The categories introduced here are therefore not to be understood as a strict taxonomy, but rather as heuristic devices that help illuminate the structural dynamics of data toxicality.

A. Directly Harmful Effects of Data

Direct harm primarily arises in situations where personal, security-sensitive, or otherwise confidential data – to borrow a common somatic metaphor in this context – "falls into the wrong hands" and is deliberately used to cause harm to individuals, businesses, or institutions. Such misuse of data is often preceded by theft of the data, carried out through techniques such as phishing, snarfing, pharming, or spoofing. The motives behind such acts vary widely. While some are primarily financially driven, aiming to extort ransom or hush money, others are explicitly intent on discrediting or misleading a target, thereby inflicting psychological or social harm – even if financial loss is consciously accepted as a collateral consequence.

Personal data can also be weaponized – not merely stolen but strategically deployed as a tool of harm. This occurs, for example, when data is made public without the knowledge or consent of those affected, with the intention of humiliating or intimidating them – as seen in the practice of doxxing (Douglas 2016, 199). This form of digital violence is particularly directed at public figures, journalists, and former romantic partners. It is also frequently used against representatives of opposing ideological positions and can be carried out by individuals and collective groups. In such cases, data is not only "in the wrong hands," but also "in the wrong place."

This notion that data can have harmful effects simply by being in an improper location makes it comparable to dirt, as understood in British anthropologist Mary Douglas's broader, symbolic definition. According to Douglas, dirt is best understood as "matter out of place" (Douglas 1966, 36) – something that is not where it belongs. This concept presupposes both an underlying order and a transgression against that order, making dirt an inherently relative concept. Dirt is never an isolated entity; it always exists in relation to a system of order that defines and excludes it (Douglas 1966, 41).

Furthermore, Douglas asserts that this system itself is underpinned by a shared social imaginary: the symbolic and conceptual frameworks through which communities interpret and "position" matter. "Shoes are not dirty in themselves, but it is dirty to place them on the dining-table" (Douglas 1966, 36). The metaphorical parallel between data and dirt, though not to be taken too far, aptly captures the moral ambivalence of data – namely, its capacity to be both empowering and harmful, depending on the context.[5]

Data can also become toxical when it is manipulated or falsified – to extend the earlier metaphor: when it becomes "contaminated." A defining characteristic of data tampering is that the data is not just stolen but deliberately altered in place. These modifications can be extremely subtle, sometimes as minor as altering a single pixel in an image (Alberti et al. 2019), making them exceptionally difficult to detect. However, even these minimal distortions can cause significant harm, particularly in fields such as financial reporting and corporate accounting, where breaches of data integrity can have far-reaching economic and societal consequences.

The potentially catastrophic impact of even minor disruptions to data integrity highlights the importance of the influential thesis of Japanese economist Hiroyuki Itami, who argued that a company's most valuable assets are invisible (Itami 1987, 12f.). The widely held belief that data, particularly in terms of its monetization, management and processing, represents the most critical corporate asset of the future must therefore be reconsidered. Data is not only an invaluable resource, but also one of the most dangerous and endangered, requiring robust protection and proactive safeguards. In this regard, the oft-quoted management adage that "what gets measured gets managed" (Fanshawe 2022, 42f.) remains highly pertinent, especially in the era of Big Data. The imperative to uphold the highest standards of data integrity is thus a foundational principle of responsible research. Alongside data quality, which also includes considerations of fairness and equity in usage, it is a *conditio sine qua non* for sound scientific practice. Violations of data integrity can result not only from insufficient verification of data sources, but also from ambiguous, outdated, redundant, or internally inconsistent datasets.

[5] Moreover, just as the harmfulness of "dirt" presupposes a purity/impurity dichotomy within a moral order (see Charles Taylor's notion of "modern moral order"), so too do misplaced data exert harm only insofar as they are judged "impure" within the socio-technical regime that defines proper informational domains.

The preceding discussion of direct harms – whether through theft, exposure, or tampering – illustrates that data toxicality operates not only interpersonally, but also on a societal scale. As the Oxford philosopher Carissa Véliz (2021, 107 – 139) compellingly argues through historical and contemporary examples, the mishandling of personal data can pose existential threats by endangering national security, corrupting representative democratic systems, and exacerbating the meaning and identity crises of liberal societies. These dynamics demand a fundamental rethinking of data governance, as the misuse of personal data drives social harm and amplifies structural crises.

These considerations already hint at the next crucial question: To what extent can data cause indirect harm? The examples of indirect harms explored in the next section are just as consequential as the direct ones discussed above. In fact, they may be even more insidious because they unfold gradually and imperceptibly, rendering their impact all the more profound and enduring.

B. Indirectly Harmful Effects of Data

Understanding the indirect harms of data – harms that are less tangible or traceable than direct ones, and potentially more far-reaching – requires acknowledging that we generate digital traces with virtually every online interaction and use of digital services, often without deliberate intent or even awareness. As Stampfl (2012, 394; translation mine) aptly describes, these data traces "sketch a digital image of our lives," providing third parties with unprecedented opportunities for control, surveillance, security enforcement, and crime prevention. At the same time, when these traces are aggregated and analyzed systematically to create behavioral, consumption, or movement profiles, they can yield profound insights into an individual's character traits, social affiliations, and interpersonal relationships – a capability of digital data that would have been scarcely imaginable only a few years ago.

These individually traceable data points, generated when entering the online world (insofar as no proxy servers or anonymization technologies are used) through IP addresses, cookies, search queries, hardware and browser settings, operating systems, installed software and more, constitute what is often called a person's digital footprint. "Unlike footprints in the sand, digital traces in silica are not wiped away by the tide; instead, they accrete, leaving incredibly detailed records of social interaction" (Welser et al. 2008, 117; original emphasis omitted). Far from being trivial by-products, these unintentionally or unconsciously generated digital residues represent highly valuable raw material for third parties. Through data-driven technologies, these traces can be extracted, repurposed, and monetized – often with little or no regard for their original context or intent. Consequently, even seemingly cost-free participation in digital life can come at a steep price: *data non sunt gratis data* – data are not given "for free."

Analogous to the undesirable side effects of mineral extraction, the collection, analysis, and processing of vast amounts of data can have negative real-world consequences for individuals and society alike. Recent analyses estimate that the ICT sector accounts for roughly 1.5 – 3% of global greenhouse gas emissions (Bieser et al. 2023). According to the International Energy Agency (IEA), this footprint is set to grow, particularly with the expansion of cloud computing and AI. If current trends continue, electricity consumption by global data centers is projected to nearly double from 2020 levels, reaching about 945 TWh by 2030 – equivalent to nearly 3% of global electricity use (Moss 2024).

Danish communication scholar Nanna Bonde Thylstrup argues that digital data traces are not ethically neutral phenomena; they are a form of digital pollution, operating according to an extractive economic logic while retaining the imprint of the bodies and behaviors from which they stem (Thylstrup 2019, 2, 4). More broadly, Thylstrup contends that the logic of datafication is fundamentally based "on a logic of waste and recycling, with significant implications for how we consider datafication's politics and ethics" (1). Building on Sarah Myers West's analysis, Thylstrup further explains that the commercialization of data establishes a logic of data capitalism that prioritizes the power of networks over traditional economic, political, and social dimensions. This is achieved by extracting value from the digital traces generated within these networks (Thylstrup 2019, 2; see also West 2019, 21). This perspective bears a strong affinity to the concept of "surveillance capitalism" developed by Shoshana Zuboff, who defines it as "a new economic order that claims human experience as free raw material for hidden commercial practices of extraction, prediction, and sales" (Zuboff 2019, iv). Another critical issue beyond this data-capitalist value chain is the intentional overproduction of data by data-intensive corporations, which generates and perpetuates what has been termed "organizational ignorance" (Schwarzkopf 2020, 197; translation mine). This phenomenon becomes particularly salient when data is framed as the strategic resource of the present era – the oft-cited "new oil" (Spitz 2017, 9) – and data ecosystems are portrayed as "Driver for Innovation and Growth" (ISST 2019, 5).

The datafication of life risks becoming a self-imposed trap when the illusion of digital freedom comes at the cost of real-world unfreedom. This is particularly true when individuals are systematically deprived of digital self-determination, including cases where such deprivation is masked as freedom of choice (e.g., through manipulative interface design or so-called "dark patterns"), thereby not only hindering, but structurally undermining their ability to realize their full personal and existential potential. This calls for an updated conceptualization of structural violence (Galtung 1969, 168) in the digital age – one that considers the pervasive surveillance made possible by extensive digital interconnectedness.[6] What once seemed like Orwellian fiction is now an all-too-real danger: the ubiquitous monitoring of human beings, extending to emotional and cognitive domains. In short, this raises the specter of a "digital dictatorship" (Schlumberger 2024, 761), whose early manifestations can be observed not only in authoritarian regimes but also in so-called "free world" democracies.

What must be acknowledged is the fundamental ambivalence that pervades human existence – an ambivalence that also characterizes the rapid development of information and communication technologies. With every technological breakthrough, new possibilities arise for constructive, life-enhancing applications, yet simultaneously, new avenues open for surveillance, oppression, and harm. This dual nature of technological progress calls for a balanced perspective: neither naïve optimism nor blanket rejection is appropriate. Just as skepticism, when pursued as a theory of knowledge, tends to be rather unfruitful (Kierkegaard 1990 [1838], 80), a purely negative stance in digital ethics risk being equally unproductive.

The final section therefore offers brief but targeted conceptual reflections on how data-related harms might be mitigated – or even constructively reconfigured – from a techno-philosophical standpoint.

III. Being Forgotten Through Unfindability

Just as biochemical toxicity cannot simply be eliminated, but rather must be managed and mitigated, we must consider how to counteract the harmful effects of data on human coexistence. In light of the previously discussed phenomena of data toxicality, this challenge is not merely theoretical, but also practical and ethical. Given the scale of digital infrastructure, debating whether

[6] One could argue that digital structural violence – understood as the systemic denial of rights and autonomy through pervasive surveillance and data exploitation – fulfills the key criteria for self-defense: it constitutes an ongoing, unjust attack on individuals' agency, and proportionate countermeasures (e.g., encryption, privacy-enhancing technologies, legal action) serve to repel that attack and restore informational self-determination. I thank Aaron J. Butler for this remark!

data should be collected and stored at all is a futile endeavor. A blanket ban on data collection, particularly of personal data, would be politically and practically unfeasible, and would eliminate not only potential harms but also valuable benefits. Therefore, the focus should shift from the question of *whether* data should be collected and stored to *how* data of different types and complexities ought to be managed – retrospectively, presently, and prospectively. This brings encryption, access controls, and the question of data deletion and its feasibility into focus.

While this discussion does not aim to provide a comprehensive analysis of the "right to be forgotten" under Article 17 of the EU's General Data Protection Regulation (GDPR),[7] it is relevant in that it addresses the issue of data deletion, which stands as a central – though not exhaustive – remedy for direct data harm, such as theft, malicious publication, or falsification. Ensuring the possibility and execution of data deletion is essential for both preventing harm and for mitigating damages already inflicted. Two fundamental questions arise: (1) What does deletion actually mean? (2) How can deletion be effectively implemented – particularly in cases involving toxical data?

Regarding the first question, it is important to note that the term "right to be forgotten" – often misleadingly shortened in discourse to "right to forget" – designates an active, selective process that mirrors the active and constructive nature of remembering (*anámnesis*, ανάμνησις), as opposed to the passivity of mere memory (*mnḗmē*, μνήμη), albeit in an inverted mode. Unlike everyday notions of forgetting, where something fades over time, the right to be forgotten does not denote a passive, natural process where data gradually disappears. Rather, it denotes the result of a deliberately guided and systematically executed process of deletion. Whether "deletion" means total eradication, contextual removal, or displacement, the right to be forgotten demands prompt and effective action. For personal data, this means not only erasing the data at its point of origin but also removing all instances, copies, links, and replications of the data (Article 17(2) GDPR). Thus, in its legal interpretation, limiting access does not constitute deletion (Abbt 2016, 353), but rather, the data must be removed from all storage, archive, and access points (Buchner 2020, 307). In short, the aim is to eradicate the data and its remnants from the digital sphere entirely (Herbst 2020, margin no. 49; cited in Buchner 2020, 307).

[7] The Regulation (EU) 2016/679 (General Data Protection Regulation) as published in OJ L 119, 4 May 2016 is available at: https://t1p.de/42y3 (Visited 25.04.2025).

However, when considering the *implementation* of deletion processes, a fundamental question arises: Does deletion still have a future in an increasingly digital world? In an era of constant data deluge and informational excess, driven by the rapid advancements in information and communication technologies, is deletion still feasible – or even conceptually tenable? Or should we regard it as a "utopia of modernity" (Hunzinger 2018, 213; translation mine)?

The complete deletion of data, including all residual traces, appears virtually impossible within the current structure of the internet. Even if the right to be forgotten were enshrined as a "human" or "digital fundamental right," the practical enforcement of such a right would remain unresolved. The prevailing discourse on the right to be forgotten repeatedly emphasizes a crucial obstacle: "The internet never forgets." Unlike physically destroying storage media, which renders data permanently unusable, disconnecting the internet is not an option. Furthermore, such measures would contradict the very logic of digital archiving (Stäheli 2021, 416), wherein even the deletion process can leave residues, such as metadata, that must also be erased, theoretically leading to an infinite regress.

Thus, while the right to be forgotten is normatively valid, it remains elusive in practice. This challenge is even more acute in the case of toxical data, which leaves lasting imprints not just online, but also in offline contexts. Addressing toxical data demands not just digital deletion but also neutralizing of its analog consequences – a task of even greater complexity. A theoretically promising solution lies in reframing the concept of deletion itself. Given the previously discussed reality that we leave behind traceable digital footprints at every turn, deletion cannot realistically aim for total erasure. Instead, the goal should be to interrupt the retrievability of data at "the right point" with surgical precision to prevent rediscovery. In short, "deletion" in the digital sphere does not imply "the (ultimately impossible) physical erasure of data traces but rather rendering them unlocatable" (Stäheli 2021, 416; translation mine). When deletion is unattainable, *unfindability* becomes its functional equivalent – and one viable realization of the right to be forgotten.

In *Sociology of Disconnection* (2021), Swiss sociologist Urs Stäheli argues that the concept of "unfindability" (irretrievability) as a "third category between storage and deletion" (417; translation mine) can be traced back to proposals from the early 1990s for the "'composting' of redundant data." Unlike digital archives designed for preservation, where the greatest risk is the inability to locate stored data, systems designed around "disconnected data" operate differently. In such a model, "individual elements, such as links or forms, remain functional but are now detached from any intelligible context" (Stäheli 2021, 417). As a result, the data is still stored but can no longer be searched or meaningfully retrieved. Given the practical challenges of deleting data, the concept of unfindability offers a compelling alternative.

To further illustrate this concept, consider the following cinematic example. At the end of *Raiders of the Lost Ark* (1981), university curator Brody asks American officials where the Ark of the Covenant – the Old Testament relic of immeasurable value and power that Dr. Jones had saved from falling into Nazi hands – has been taken. Major Eaton reassures him that it is "somewhere very safe" so that top specialists can examine it. In the iconic final scene, a warehouse worker seals the Ark inside a plain wooden crate bearing the label: "Top Secret Army Intel 9906753 – Do Not Open!" Secured with only a simple padlock, the crate is placed in an endless labyrinth of identical wooden boxes and vanishes into an infinite storage labyrinth.

While the many interpretations of this famous ending are not our concern here, I draw on an interpretation by Rainer Erlinger (2019, 127 – 132) that offers a compelling metaphor for how unfindability applies to toxical data when transposed to our context. Indeed, the Ark, an object of unparalleled value and extraordinary power, is placed in an extremely secure location by being submerged within a sea of sameness, rendering any retrieval effort functionally and/or effectively futile. The safest place to hide something is not always a specific location, but rather an entirely indeterminate one. "It suffices to produce so many other crates that one has almost no chance of finding the one crate containing the truth – or, even if one does find it, of recognizing it with certainty. Truth is merely one piece of information among many, differing only in that it corresponds to reality. But from the outside, one cannot necessarily tell the difference." (Erlinger 2019, 128f.)

Can this theoretical construct – essentially a digital form of intentional misfiling – be operationalized as a means of countering data toxicality? Clearly, operationalizing unfindability presents substantial challenges of its own. Simply hiding data within an enormous repository of other data may reduce its accessibility but does not eliminate its existence. In other words, simply burying data in volume may obfuscate, but does not annihilate.[8] One could

[8] This logic echoes a classic literary example: in Edgar Allan Poe's *The Purloined Letter* (1844), a stolen document remains undetected precisely because it is hidden in plain sight – among

implement unfindability via a "noisy-scattering" strategy involving the injection of random noise, false records, and the fragmentation of genuine content into decoy "pieces." By flooding the archive with both authentic and counterfeit fragments (think of a jigsaw puzzle whose real pieces are hidden among hundreds of fakes), this method exploits signal detection theory by overwhelming search attempts with false positives.[9] Unlike absolute deletion, however, unfindability is susceptible to evolving search techniques, algorithmic improvements, and technological advances.[10] Nevertheless, given the growing limitations of deletion, unfindability offers a conceptually and technically plausible path forward – one that works with, rather than against, the archival logic of the digital realm.

other, seemingly ordinary papers. Similarly, data embedded within a mass of similarly mundane or unremarkable information may evade discovery not through encryption, but through contextual camouflage.

[9] I am again grateful to Aaron J. Butler for this remark!

[10] In the age of AI, the *practical* viability of unfindability becomes even more questionable: advanced models capable of inference, correlation, and reconstruction from partial data may ultimately discover even well-hidden information. Ever-improving neural search and pattern-completion architectures can retrieve meaning from fragmented traces – suggesting the need for a kind of digital counterpart to the so-called "Neuralyzer," a fictional device featured in the 1997 American science-fiction film *Men in Black*. Two counterstrategies appear promising: (a) *Textual or dataset poisoning*: this technique introduces imperceptible alterations into data to deceive AI models while remaining intelligible to humans. Such perturbations may involve lexical interference, semantic distortion, or encryption-like encoding. However, this method presupposes knowledge of the model's internal structure. If one seeks to "poison" a known model – say, of type XYZ – then the perturbations can be targeted, much like the technique used in the Nightshade tool. Yet if the goal is to render data unfindable in general, across models like XYZ, XYZ2, or a hypothetical XYZ3 that may be developed two decades from now, the problem becomes much harder. One cannot yet anticipate how a future system will "think," let alone how it might be misled. I thank Piet Jarmatz for this critical remark! (b) *Decentralized proliferation of altered copies*: this technical strategy shifts the emphasis from deletion to dilution. By flooding the digital environment with multiple, modified versions of sensitive data, it becomes increasingly difficult to reconstruct a singular, coherent "truth." This approach undermines the pattern recognition capabilities of AI systems by saturating the informational space with ambiguity. Both theoretical strategies aim not to erase data entirely, but to render it effectively irretrievable – even by systems optimized to detect signals amid noise and incompleteness. A more detailed exploration of these strategies will follow elsewhere.

Bibliography

ABBT, C. (2016): *Ich vergesse. Über Möglichkeiten und Grenzen des Denkens aus philosophischer Perspektive*. Frankfurt am Main: Campus.

ALBERTI, M. et al. (2018): Are You Tampering with My Data? In: *Proceedings of the European Conference on Computer Vision (ECCV) Workshops.* Available at: https://arxiv.org/abs/1808.06809 (Accessed 25 April 2025).

BIESER, J. C. T. – HINTEMANN, R. et al. (2023): A Review of Assessments of the Greenhouse Gas Footprint and Abatement Potential of Information and Communication Technology. *Environmental Impact Assessment Review*, 99, 107033, 1 – 12. DOI: https://doi.org/10.1016/j.eiar.2022.107033

BUCHNER, B. (2020): Grundsätze des Datenschutzrechts. In: Tinnefeld, M.-T. et al. (eds.): *Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht.* 7th ed. Berlin and Boston: De Gruyter Oldenbourg, 220 – 332.

DOUGLAS, D. M. (2016): Doxing: A Conceptual Analysis. *Ethics and Information Technology*, 18 (3), 199 – 210. DOI: https://doi.org/10.1007/s10676-016-9406-0

DOUGLAS, M. (1966): *Purity and Danger: An Analysis of Concepts of Pollution and Taboo.* London: Routledge.

ERLINGER, R. (2019): *Warum die Wahrheit sagen?* Frankfurt am Main: Fischer.

FANSHAWE, S. (2022): *The Power of Difference: Where the Complexities of Diversity and Inclusion Meet Practical Solutions.* London et al.: Kogan Page.

GALTUNG, J. (1969): Violence, Peace, and Peace Research. *Journal of Peace Research*, 6 (3), 167 – 191.

GENNERMANN, P. (2020): Call for Papers 2020. Available at: https://t1p.de/w6wr2 (Accessed 25 April 2025).

HERBST, T. (2020): Art. 17 Recht auf Löschung ("Recht auf Vergessenwerden"). In: Kühling, J. – Buchner, B. (eds.): *Datenschutz-Grundverordnung BDSG. Kommentar.* 3rd ed. Munich: C.H. Beck, 499 – 527.

HUNZINGER, S. (2018): *Das Löschen im Datenschutzrecht.* Baden-Baden: Nomos.

ISST [Fraunhofer Institute for Software and Systems Engineering] (2019): *Data Ecosystems-Conceptual Foundations, Constituents and Recommendations for Action*. Available at: https://t1p.de/1nzkr (Accessed 25 April 2025).

ITAMI, H. (1987): *Mobilising Invisible Assets.* Cambridge, Massachusetts: Harvard University Press.

KIERKEGAARD, S. (1990 [1838]): *From the Papers of One Still Living*. In: *Early Polemical Writings*. Ed. and trans. by J. Watkin. Princeton, New Jersey: Princeton University Press, 53 – 102.

MOSS, S. (2024): *Global Data Center Electricity Consumption*. Available at: https://t1p.de/ts3sy (Accessed 25 April 2025)

MYERS WEST, S. (2019): Data Capitalism. Redefining the Logics of Surveillance and Privacy. In: *Business & Society* 58 (1), 20 – 41. DOI: https://doi.org/10.1177/0007650317718185

PARACELSUS (1928): Sieben Defensiones. In: *Theophrast von Hohenheim gen. Paracelsus: Sämtliche Werke*. Ed. by K. Sudhoff, Tome 1. *Medizinische, naturwissenschaftliche und philosophische Schriften*, vol. 11, *Schriftwerk aus den Jahren 1537 – 1541*. Munich and Berlin: R. Oldenbourg, 123 – 160.

PASSOW, F. (1825): *Johann Gottlob Schneiders Handwörterbuch der Griechischen Sprache*, vol. 2., 3rd ed. Leipzig: Vogel.

PFEIFER, W. (1989): *Etymologisches Wörterbuch des Deutschen*, vols. 1 – 3. Berlin: Akademie-Verlag.

SCHLUMBERGER, O. et al. (2024): How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition*, 59 (3), 761 – 783. DOI: https://doi.org/10.1017/gov.2023.20

SCHREIBER, G. (2022a): *Im Dunkel der Sexualität. Sexualität und Gewalt aus sexualethischer Perspektive.* Berlin and Boston: De Gruyter.

SCHREIBER, G. (2022b): Datentoxikalität. Eine technikethische Herausforderung. In: Augsberg, S. – Gehring P. (eds.): *Datensouveränität: Positionen zur Debatte*. Frankfurt am Main and New York: Campus, 199 – 217.

SCHREIBER, G. (2024): Reconsidering Agency in the Age of AI. *Filozofia*, 79 (5), 529 – 537. DOI: DOI: https://doi.org/10.31577/filozofia.2024.79.5.5

SCHWARZKOPF, S. (2020): Sacred Excess: Organizational Ignorance in an Age of Toxic Data. *Organization Studies*, 41 (2), 197 – 217. DOI: https://doi.org/10.1177/0170840618815527

SPITZ, M. (2017): *Daten – das Öl des 21. Jahrhunderts? Nachhaltigkeit im digitalen Zeitalter.* Hamburg: Hoffmann und Campe.

STÄHELI, U. (2021): *Soziologie der Entnetzung.* Berlin: Suhrkamp.

STAMPFL, N. S. (2012): Leben im digitalen Panopticon. *Scheidewege: Jahresschrift für skeptisches Denken*, 42 (2012/2013), 393 – 405.

THYLSTRUP, N. B. (2019): Data out of Place: Toxic Traces and the Politics of Recycling. *Big Data & Society*, 6 (2), 1 – 9. DOI: https://doi.org/10.1177/2053951719875479

VÉLIZ, C. (2021): *Privacy is Power: Why and How You Should Take Back Control of Your Data.* London: Penguin Random House.

WELSER, H. T. et al. (2008): Distilling Digital Traces. In: Fielding, N. et al. (eds.): *The SAGE Handbook of Online Research Methods.* London et al.: Sage, 116 – 140.

ZUBOFF, S. (2019): *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.

Gerhard Schreiber
Faculty of Humanities and Social Sciences
Helmut Schmidt University/University of the Federal Armed Forces Hamburg
Holstenhofweg 85
22043 Hamburg
Germany
e-mail: schreiber@hsu-hh.de
ORCID ID: https://orcid.org/0000-0003-1178-1802