societies

MDPI

Article

What Counts as "People" in Digital Social Research? Subject Rethinking and Its Ethical Consequences

Francesca Romana Lenzi [1,*], Angela Delli Paoli [2] and Maria Carmela Catone [3,*]

[1] Department of Movement, Human and Health Sciences, University of Rome "Foro Italico", 00135 Rome, Italy
[2] Department of Humanities, Philosophy and Education, University of Salerno, 84084 Fisciano, Italy; adellipaoli@unisa.it
[3] Department of Social and Political Sciences, University of Salerno, 84084 Fisciano, Italy
* Correspondence: francescaromana.lenzi@uniroma4.it (F.R.L.); mcatone@unisa.it (M.C.C.)

Abstract

This article examines how digitalization reshapes the research subject in social inquiry. We ask, "What counts as a research subject in digital social research, and how do we ethically account for people represented through data, traces, and algorithmic profiles?" We argue that data are inseparable from the people who produce and are affected by them and describe a three-pronged separation—between data and persons, persons and bodies, and researchers and persons—that risks dehumanization. Drawing on examples of native and digitized data and on voluntary, unintentional, and infrastructural traces, we map key harms, including privacy breaches, dataveillance, manipulation, and discrimination. We then revisit core ethical principles—consent, anonymity, and confidentiality—considering open science and platform-mediated environments, and highlight the role of algorithmic awareness. The paper offers a conceptual reframing of the "subject" in digital social research and provides a set of practical implications for responsible practices. We conclude with recommendations to re-humanize data through relational ethics, transparent methods, and participant education.

Keywords: digital social research; datafication; research ethics; human-data relations; epistemology of digital methods

Academic Editors: Cristóbal Fernández-Muñoz and Eugène Loos

Received: 15 July 2025
Revised: 10 November 2025
Accepted: 12 November 2025
Published: 26 November 2025

Citation: Lenzi, F.R.; Delli Paoli, A.; Catone, M.C. What Counts as "People" in Digital Social Research? Subject Rethinking and Its Ethical Consequences. *Societies* **2025**, *15*, 329. https://doi.org/10.3390/soc15120329

1. Introduction

Recent and ongoing technological innovations are creating both opportunities and challenges for social research by providing access to new forms of data and enabling the development of novel methods and analytical techniques. Digital social research can be broadly defined as the study of social phenomena in digital spaces, utilizing digital technologies and data, and emerging from the complex interplay between methodological approaches, technological tools, digital environments, and social life itself [1,2]. It spans multiple levels of social life—micro, meso, and macro—impacting areas such as citizenship, identity, power, inequalities, and social networks. From a methodological perspective, this approach enables the collection and analysis of digital traces and computer-mediated interactions, offering new opportunities for social research while presenting significant epistemological challenges.

While acknowledging that digital social research raises a wide range of theoretical and methodological issues, which have been extensively addressed in previous contributions [2–5] this paper aims to highlight its consequences for, and impacts on,

people. The role of individuals in the production and analysis of digital data has undergone profound changes; for instance, people are increasingly becoming unwitting data sources rather than active participants. This shift is accompanied by new forms of exposure, surveillance, and algorithmic categorization, which can generate vulnerabilities and reinforce existing inequalities. In this context, researchers in the social sciences face new responsibilities as they must critically reflect on their methodological approaches, tools, and the ethical conditions that shape the observation of social phenomena within and through digital environments.

To this end, at the center of our analysis, we place one explicit main research question (MRQ) and two supporting questions:

MRQ: What counts as a research subject in digital social research?

RQ1: What risks does this pose for people?

RQ2: How should research ethics adapt to digital contexts?

This paper is organized as follows. The Section 1 explores digital data in relation to people investigating the nature of digital data and their implications for people, mainly deriving from the separation between data and people, between people and bodies, and between people and researchers. The Section 2 classifies the risks deriving from digital social research to people according to the types of digital violations of rights. The last section analyses ethical challenges to traditional social research principles and proposes solutions. In the final section, the main findings are discussed, and conclusions are drawn.

2. Digital Traces and the Abstraction of People

To address the main research question, we first clarify what counts as empirical material in digital social research.

The variability of empirical material stems from two dimensions—(1) production, encompassing information created within digital environments (native) versus information digitized from offline sources, and (2) mode, spanning information elicited by the researcher (provoked) versus information produced without intervention (unprovoked).

Distinctions related to the nature of information also include those related to its research design, operationalization, and coding. *Provoked information*, requested by a researcher, is the result of one's research design and conceptual and operational definition, being subjected to a coding process that allows for its inclusion in a case-by-variable matrix. For this reason, such data can be called digital "data." In contrast, unsolicited information disregards the case-by-variable matrix in the same way as interview transcripts, and for that reason, such data can be called digital "traces".

Digital traces are specific, natively digital resources that constitute an empirical basis that cannot be traced to any other type available in traditional social research.

They are information produced routinely as a result of the incorporation of digital technology into our daily lives, social lives, and everyday practices.

Data generation can be voluntary, for example, through user-generated online content (social data)—profiles and accounts, texts, comments, posts, images, videos, and interactions on social media, communities, blogs, and groups—or through our browsing behavior, such as search engine queries, clicks on links, and visits to websites.

It can also be involuntary, such as when transactional traces arise from the ubiquitous use of devices [6]), including automatic logs of operations carried out with connected devices (smartphones, PCs, tablets) or via digital identities, credit cards, and purchase cards; footprints created by the Internet of Things (that is, objects equipped with sensors and software able to transmit/receive data and automate actions (home automation for lighting and climate control, monitoring of energy consumption, remote security systems, driver-assistance systems, smart energy grids, telemedicine, sensors in public spaces);

records kept by hospitals and other service providers; geospatial data originating from GPS technology; and self-generated lifelogging from smartphones, apps, and wearable devices (e.g., smartwatches and fitness trackers), including online games.

The main ethical challenge of using these traces for research derives from a *triple distance*. The first type of separation is between data and persons. The second type of separation is between persons and bodies. The third type of separation is between researchers and persons. To explain the first type of separation, we can consider, for example, the factual traces of human activities, practices, and relationships, such as in the case of big data: data from GPS capable of tracking the physical movements of people towards gyms over long periods, or data recorded from fitness and wellness apps that can provide information about the type and frequency of exercise, sedentary lifestyles, eating habits, etc. A variety of areas can be intentionally or unintentionally tracked (e.g., sleep quality, weight, energy levels, mood, cognitive performance). Various self-tracking tools, such as emotion trackers, food trackers, pedometers, GPS, and wearable devices, transform people into metrics, a series of quantifications that can be analyzed, examined, and acted upon. The metaphor of the quantified self, which represents the self in metrics, figures the self as a more intelligent machine that, like machines, can be extended and enhanced if needed [7]). The quantified self metaphor views tracking as a powerful tool for understanding oneself and gaining control over one's life. Automatically recorded data allows for the collection of very detailed, factual, and behavioral information that is hard to gather with traditional methods. For example, consider measuring sports practices or eating habits. To find these through survey questions, one might ask about the frequency of sports, whether they go to the gym, how often they exercise, or the number of hours they spend on activities. Besides the limited number of people who can answer such questions, there are cognitive and memory challenges—like difficulty recalling past actions or calculating how often they occur in hours or days—and challenges in articulating behaviors, thoughts, and opinions. Conversely, digital traces from GPS, fitness apps, or wearable devices can provide detailed information about daily physical activity, its frequency, sedentary time, and heart rate patterns. They can also monitor the daily movements of many people over long periods, from their homes to gyms. Self-representation is increasingly transformed into a numerical enterprise that does not require words or narrative; emotions, moods, and mental states need not be consciously expressed linguistically but can be inferred from bodily indicators—such as stress monitoring and heart rate variability—and from online content, including posts and comments [8,9]. As Rudder puts it, "the idea is to move our understanding of ourselves away from narratives and toward numbers, or, rather, to think in such a way that numbers are the narrative" [10]. Self-work is no longer a conscious act but an automated bodily function. Some interpret this shift as a somatization of the person, insofar as the body and its health manifestations become the key site of self-work [11]. In this context, the hermeneutic constitution of the self, as a thinking (and not merely conative) act, collapses, being replaced by the immediacy of numbers [12].

It is true that, unlike "provoked" information, digital traces are largely naturalistic and non-intrusive, because individuals do not modify their opinions and behaviors in response to being observed or questioned. However, prior research has problematized the naturalistic character of digital data, pointing to presentational strategies that, even online, mirror the social desirability tendency [13]. Moreover, unlike information elicited through direct questioning, digital traces are not always conscious. When responding to a question, a person deliberately positions themselves with respect to the answer; this is not the case with digital information.

Individuals become passive agents within digital information ecologies and struggle to understand the traces and footprints they unknowingly produce. They interpret them

as a partial and superficial representation of themselves, as not the real them [14], as a digital subject, an abstract and performative persona built through data, profiles, and other records and aggregates [15].

When intentionally created (e.g., autobiographical posts and comments), such traces create another separation (the second type of separation), between people and bodies. Digital identities are often disembodied; sometimes, they may serve as a way to escape the limits of embodied bodies and contexts. Digital traces are unreliable as straightforward proxies for physical identity. Online texts, images, and interactions are typically curated to fit an idealized self, consistent with Goffman's account of impression management [16]. In online communities, identity often exceeds corporeal boundaries, creating a gap between bodies and digital personas. For researchers, attempts to "triangulate" virtual and offline selves risk importing the presumed truths of the corporeal world into digital contexts and, in doing so, undervaluing the digital self as a legitimate—and sometimes preferable—mode of non-normative self-expression.

A clear example is the well-known case of David and Amy Taylor. Despite offline circumstances, they created successful, slim avatars in Second Life; Amy's discovery of David's virtual affair led to their marriage breakdown [17]. The issue is not the discrepancy itself but its consequences. Digital selves—whether embodied or not, "true" or "false"—can have tangible effects in the real world.

The "found," non-provoked nature of digital data introduces a third kind of separation, namely that between data and researchers. Because such data can be collected without interfering in people's lives, researchers access private information through layers of mediation—social media profiles, data systems, algorithms, and transaction logs—rather than through direct interaction. This reduces the perception of the human subject and turns digital social research into a mostly one-directional collection of data, conflicting with the participatory ideal of social inquiry. The result is both epistemic and ethical: it hampers deep understanding while undermining trust, relationships, dialog, and the collaborative creation of knowledge. Without an emotional researcher–participant connection, ethical issues can easily develop [18]. Researchers are often left to interpret intentions and decide how to handle data, frequently assuming that making data public means it can be used legitimately. However, privacy expectations often surpass legal standards—even in public spaces, individuals may expect privacy, and researchers might unintentionally breach those expectations [19].

Overall, the three-pronged separation between data and subjects, bodies and subjects, and researchers and subjects obscures ethical concerns, spreads responsibility and accountability by weakening the link between data and people, and tends to lead to an overemphasis on bodies within disembodied digital identities. They blur the line between data and individuals, especially in large-scale studies lacking direct one-to-one interaction, and challenge assumptions about the difference between data generated by people and people themselves [20].

While earlier metaphors such as the "quantified self" [7] stressed risks of reducing humans to metrics, more recent studies [11,12] emphasize the socio-technical assemblages in which data are embedded. These hybrid framings move beyond strict dichotomies between people and data.

Individuals are fragmented into scattered traces—a transmogrification into constellations of abstracted data points detached from context and lived experience [21]—which then appear untethered from their creators and are treated as ontologically separate. Being based on traces, digital social research assumes the nature of text-based research instead of human-based research. This would legitimize glossing over the ethical issues: with docu-

ments, footprints, and traces, and not people, it is not necessary to provide protection. By removing people from the research process, ethical protocols would become superfluous.

However, digital traces cannot be considered cultural products or artifacts; rather, they are autobiographic texts, presentations, and representations of human identities, opinions, activities, and behaviors.

Using digital traces as documents, we risk dehumanizing the individuals behind posts, comments, and footprints [22]. To highlight the presence of people in digital data and the potential harms that may arise from their primary and secondary use, Metcalf and Crawford [23] use the term "data subjectivity." Similarly, Zook et al. [24] recognize the first (out of 10) rule of responsible digital research as the acknowledgment that data are people and can cause harm.

While Metcalf and Crawford [23] first called for consolidated frameworks, subsequent work [25–27] shows how regulation has since evolved. Despite GDPR and related reforms, many challenges remain, suggesting their insights are still relevant but require reinterpretation in 2025.

3. Framing Risks to Individuals in Digital Research

We can identify several families of risks relevant to digital social research ethics, as recognized in the literature, relative to different stages of the research design.

The first one emerges both at the data collection and the finding presentation and dissemination stages. It is the "Digital Privacy" risk, which consists of collecting private or sensitive information and/or unintentional information (information people are not aware of) and/or divulging expected private information. The collection and analysis of personal data through techniques such as lurking [28] and scraping [29]) expose individuals to significant privacy violations, mainly due to the risk of re-identification [30] via combinations of apparently non-sensitive attributes: unintentionally neutral details, such as postal codes, may be linked to sensitive attributes like ethnicity, gender, sexual orientation, and so on. Such practices could violate individuals' right to privacy, especially without strong data protection measures. Data subjects can be profiled and monitored without their explicit consent [5].

A notable example involves the digitization of social services, where hyper-specialized service delivery can jeopardize not only users' privacy but also contributes to a form of consumer hyper-targeting driven by algorithmic profiling [31].

Fainmesser, Galeotti, and Momot [32] highlight how not all platforms are incentivized to protect user privacy. Their economic model illustrates that privacy protection is often inversely proportional to a platform's revenue strategy: the more valuable a user's data is to third parties, the weaker the privacy protections tend to be. This dynamic is especially clear in data-driven platforms (such as Facebook, Google, TikTok), which earn revenue by selling data for targeted ads. However, usage-driven platforms (like Netflix, Spotify), which generate income from subscriptions, may offer more limited privacy protections simply because they expose less data.

User behavior also plays a crucial role. Many individuals agree to terms and conditions, including the use of cookies and data processing, without fully understanding the implications. This points to a critical gap in digital literacy, which increases vulnerability to privacy violations [33].

In research, privacy can no longer be framed as a binary between public and private spaces. Instead, it must be considered in a contextual manner [34]. For example, a Facebook post set to public may be technically accessible via scraping. However, the user may not be aware that it is being used for research purposes, constituting a potential breach of privacy. This is for two main reasons.

The first issue is that the vague language used in the platforms' terms of use, which alludes to "use for research," does not require the disclosure of the specifics of a particular research program.

The second one is related to expectations of privacy, which goes beyond what is formally and legally public. Some spaces, although formally public, may be perceived as private. This is the case for some blogs or online communities where people publish diaries that are perceived as their private diaries, irrespective of their public nature. This implies that divulgation of such information by research is considered inappropriate, breaching and violating the expectations of privacy.

The assumption that public data are harmless because they do not directly affect people's lives is mistaken. Even non-identifiable information can be linked with other datasets—via pseudonyms, timestamps, or geolocation—to re-identify individuals and communities, breaching privacy and enabling racial, socioeconomic, or gender-based profiling [23]. Re-identification of "de-identified" data has occurred repeatedly.

Contemporary computing enables unprecedented scales of data collection, storage, and retention. AI further expands both intelligent data capture and analytic capacity, intensifying privacy risks and obscuring who collects which data. Some scholars characterize this environment as internet surveillance [35] or "surveillance capitalism" [36], a business model premised on data extraction, behavioral manipulation, and dependence.

For individuals, the result resembles a panopticon [37]: continuous visibility to an unseen observer induces self-discipline even without actual monitoring. While not universal, awareness of potential observation can chill expression and promote conformity, linking privacy directly to questions of freedom and democratic participation.

This broader risk is "dataveillance"—the systematic monitoring and profiling of individuals via their data records, rather than through direct observation [38].

This practice threatens individual autonomy by enabling continuous tracking of online activity, shaping decisions, narrowing choices, and constraining mobility. The 2024 Freedom on the Net report documents how surveillance and censorship—including restrictions on expression—undermine civil liberties; it highlights control tools such as geolocation that permit tracking without consent, thereby limiting freedom of movement and, by extension, autonomy.

Scholars call for robust regulatory safeguards. Metcalf and Crawford [23] argue for consolidated frameworks, while Clarke and Greenleaf [25] and Büchi, Festic, and Latzer [26] show that awareness of monitoring fosters self-censorship, altering how users communicate online due to fear of adverse consequences.

A key idea in this area is the "chilling effect," as explained by Büchi, Festic, and Latzer [26]. This describes how the perception of surveillance discourages online communication, causing users to hold back their expressions. This, in turn, impacts the quality and authenticity of information collected in social research, as well as its naturalness and spontaneity. An example given by the authors happened in the summer of 2020, when the U.S. president signed an executive order to suspend renewing temporary work visas. In this situation, a graduate student wanted to publicly share a critical opinion on X (formerly Twitter) but chose not to, fearing it could harm their future visa renewal. The student said, "I would have liked to say something about this, but I didn't, for fear it could negatively affect my visa renewal application. We shouldn't have to think about these things". This example shows how even trivial, legitimate behaviors—such as commenting on the news—can be chilled by perceived surveillance. Fearing that digital traces might be used against them, the student reduced their participation in public debate, with consequences for democratic engagement.

Lupton and Michael's [39] focus groups with 48 Australian students used creative, reflective tasks to elicit views on dataveillance. Participants displayed broad—if not always technical—awareness of data collection by platforms like Facebook and Google, often for targeted advertising. They expressed marked ambivalence—data are seen as useful for improving daily life, yet also as a source of potential misuse and intrusion.

Wearables (smartwatches, fitness trackers) were viewed as normalized and even desirable, accepted in the name of efficiency, health, and self-control. This study highlights a persistent tension between tacit acceptance of dataveillance as part of everyday digital life and discomfort with its growing invasiveness, raising questions about the line between utility and intrusion, control and surveillance, in a context of continuous data collection, aggregation, and reuse with unequal effects on life chances. Beyond curbing individual autonomy, dataveillance also compromises the trustworthiness of data, exposing it to social desirability (and undesirability) effects [13].

In addition to violating privacy and autonomy, digital research can also be used for "mass manipulation": digital footprints such as likes on social media or clicks may be used to assess people's psychological traits in order to influence their behavior and manipulate their actions (e.g., elections, business, and so on).

Another risk is what can be called "Digital Discrimination," driven by the non-neutrality and opacity of algorithms that select information. Rubinstein et al. [40] introduced the idea of digital discrimination in early debates. Since then, scholars have expanded this concept to cover algorithmic bias and systemic inequality [41,42]. Real-world cases, such as algorithmic bias in criminal justice [43], and recent discussions on AI misinformation [44], demonstrate that while the original conceptualization remains valuable, it requires updating to reflect contemporary contexts.

Continuous profiling of individuals online [40] increases risks related to the violation of personal freedoms, especially concerning the so-called "domestication" of algorithms—that is, adapting intelligent technologies to systemic goals that are not always transparent [27,44]. One well-known example is the phenomenon of filter bubbles [45,46], which are isolated informational environments that can limit users' exposure to diverse content, thus impoverishing public debate and spreading misinformation and discrimination. Decisions based on incomplete or distorted data can undermine individuals' ability to be treated fairly and to access diverse information [47]. Similarly, academic research can be influenced by these mechanisms—selection algorithms may exclude, sometimes erroneously, users or content that do not fit profiling criteria, thereby limiting the reliability and representativeness of the collected material [13,48]. The opaque algorithmic mechanisms of information selection can produce digital discrimination in the form of inequalities based on income, education, gender, age, ethnicity, and religion by overrepresenting some groups and underrepresenting others [42]. Discrimination can be direct, arising from procedures that target vulnerable, disadvantaged, minority, or non-normative groups (disabled, LGBTQ+, women, etc.), or indirect, arising from procedures that unintentionally discriminate against individuals or groups although not based on discriminatory attributes [41]. This may worsen existing inequalities, such as wealth distribution disparities, geographic inequalities, or racial inequalities, that lead to ethnic minorities being excluded from social participation. It can also create new forms of discrimination, such as economic or health discrimination. Discriminatory selection and analysis can undermine the autonomy and participation of stigmatized groups in society and violate principles of equality and fair treatment. One prominent example is the COMPAS software used in the U.S. judicial system to assess recidivism risk. An investigation by Angwin et al. [43] revealed severe racial biases: African Americans were often classified as "high risk," even with minor offenses and no criminal records, while white individuals with serious offenses were often labeled "low risk." A notable

case involves Brisha Borden, a young African American woman arrested for stealing an unattended bicycle and scooter. Despite the minor offense and lack of significant prior records, the software classified her as "high risk", whereas Vernon Prater, a white man with a history of armed robberies, was judged as "low risk". Müller [27] offers an alternative approach to aligning AI values with human societal values. Rather than trying to build "moral machines," the author suggests "domesticating" AI—similar to the historical domestication of animals—to promote regulated and responsible coexistence. Another risk, related but independent, concerns "autonomy." Algorithms can paradoxically violate autonomy: personalized content should enhance decision-making by filtering relevant information, but relevance is a subjective judgment that algorithms cannot truly make. Personalization can lead to institutional or commercial preferences dominating individual choices. Additionally, by narrowing the diversity of information (excluding what is deemed irrelevant), personalization can diminish individuals' agency and undermine autonomy [49]. The final risk involves "deception," common in digital social research yet often underestimated in terms of harm. Deception here entails covert observation or collection and analysis of digital data—people being spied on or interacting with researchers under false identities. This conflicts with honest social research, which depends on dialog and trust between people and researchers. Such deception can be considered fraud—stealing personal information and violating privacy. Table 1 summarizes the primary risks identified in digital social research analyzed herein.

Table 1. Ethical risks in digital social research.

Risk Category	Example	Recent Source
Privacy breaches	Scraping public posts without consent	Kozinets and Gambetti [28]; Zuo et al. [30]
Dataveillance	Continuous profiling of online activity	Büchi et al. [26]; Zuboff [36]
Manipulation	Microtargeted ads in elections	Fainmesser et al. [32]
Digital discrimination	Algorithmic bias in criminal justice	Angwin et al. [43] Spitale et al. [44]
Deception	Covert digital observation	Hennell et al. [50]

4. Section 3: Ethical Challenges

Starting from the research questions, we propose the concept of redefining what "counts" as a research subject (MRQ) in socio-technical terms—not only persons, but also their traces, their profiles, and the algorithmic assemblages that represent them without fully coinciding with them. This reclassification clarifies the risks (RQ1)—erosion of autonomy through pervasive dataveillance and profiling; re-identification of "anonymous" data, as well as self-censorship and inequalities in outcomes (opportunities, mobility, public voice)—and infrastructural vulnerabilities tied to opaque platforms and the tension between open science and participant protection. The ethical response (RQ2) is to shift from static rules to a situated, continuous practice that integrates iterative, participatory consent (including double or delayed consent), contextual and narrative anonymization, and confidentiality understood as a relational, as well as technical, principle (encryption, obfuscation, secure backups, organizational governance). This also calls for transparency and accountability across data supply chains, due diligence in relation to third-party infrastructures, data minimization and proportionality, impact assessments, and redress mechanisms. Finally, fostering "algorithmic awareness" among users and researchers is crucial for recognizing mediations, negotiating privacy expectations, and co-constructing rights-respecting research practices in evolving digital ecologies.

In digital social research, ethical reflection can no longer be a simple copy of traditional models. Digital data are not just 'new types of data'; they represent a significant shift in how researchers, subjects, and objects of inquiry relate to each other. This change

affects the conditions under which knowledge is created, what can be known, and the relationships involved. In this context, the ethics of social research is not just about applying existing rules, but reexamining the core principles of scientific responsibility. Researchers face mediated and elusive entities, such as digital traces that stand for individuals but are not the individuals themselves. This requires them to constantly question what it means to protect privacy, ensure transparency, and obtain informed consent. From this perspective, the complexity of digital data—together with the previously discussed three-pronged separation—poses substantial ethical challenges for digital social research. Digital traces, though not elicited by direct researcher intervention, are never neutral; they carry implications for the individuals they reference. As abstract, partial, and often disembodied representations, these traces challenge conventional frameworks of ethical protection in social inquiry.

This growing complexity becomes even more problematic due to specific features of digital environments, such as the absence of direct and participatory contact between the researcher and the subject, and the difficulty in identifying and holding accountable those who generate the data. These challenges are further amplified by the ontological instability of digital data and the socio-technical infrastructures in which they are embedded, often opaque systems that elude the full control of researchers.

Susan Halford [51] further clarifies this point, arguing that social media data are not finished products because they can be modified, deleted, or combined, which makes it difficult to ensure anonymity and consent. Moreover, their use involves multiple disciplines—such as computer science and social sciences—that often follow different ethical standards. While social sciences tend to prioritize protecting participants, hard sciences and computer science approaches are more likely to treat public data as freely usable. This disciplinary divide further complicates the ethical governance of digital research, as researchers must navigate between conflicting logics of data use, responsibility, and regulation.

Given this complex setup, it is essential to rethink the core ethical principles that support human research, especially informed consent, anonymity, and confidentiality. These principles need to be updated and rephrased to respect the individuality of data, preventing the digital and "found" nature from justifying careless research or violations of rights. Let us examine each point.

Starting with informed consent, it is crucial that participants are provided with clear, straightforward information about the main aspects of the study—methods, goals, and risks—so they can make informed choices. Participants should fully understand their role and be able to trust the researcher [50].

However, in digital settings, this becomes more complicated due to the blurred lines between public and private data, uncertainties around who owns content, and the challenge of establishing trust online—especially in "big data" research [50]. The risks mentioned earlier hinder the ability to obtain informed consent. Users are often unaware that they generate data, making it difficult to identify who is involved and in what capacity. Data surveillance involves the automated, large-scale gathering of data, often without direct contact with individuals. Additionally, deceptive tactics like covert observation or using fake identities bypass consent altogether, jeopardizing transparency in the researcher–participant relationship.

In particular, ensuring truly informed consent is especially challenging in big data contexts, where data collection often happens automatically and on a large scale, without direct interaction between the researcher and the user. As a result, consent is rarely fully informed or explicit. Even when information is provided through terms of service or privacy policies, these are usually too complex for the average user to understand.

This lack of understanding has been highlighted in numerous studies. For example, Geier et al. [52]) show that participants often skip or only skim online consent forms, while Sloan et al. [53] point out that users struggle to understand how their social media data can be linked and reused in research. Similarly, Clark et al. [54] and Hennell, Limmer and Piacentini [50] emphasize that consent in digital contexts is weak and unstable, requiring greater dynamism and transparency. From this perspective, due to the practical difficulty of obtaining consent for large datasets, researchers often avoid making the request. However, the scientific community broadly agrees on the need to maximize the protection of individuals providing data and to reflect ethically on how it is used [55,56]. In this scenario, the traditional model of informed consent—based on the idea that participants fully understand the aims of the research—is facing significant challenges. Nunan and Yenicioglu [57] identified three main issues that hinder the application of this ethical principle in digital research. The first issue is tied to involuntary data production, meaning the generation of digital traces by users without their knowledge. This data is then reused for research, raising questions about the level of awareness and intentionality behind digital communication practices and activities. Users often do not realize they are producing data that can be analyzed or used for research purposes. Second, temporality must be considered, as digital research often collects data before research questions are clearly defined. This approach makes it difficult to predict the study's objectives or communicate the purpose of data processing transparently, undermining the principle of informed consent underlying ethical approval. Third, the relational nature of participation complicates assigning individual consent in intersubjective and networked contexts, such as social media. Online interactions happen in spaces where content is co-created, shared, and referenced by multiple users simultaneously. This makes it difficult to determine who should be considered a participant and consent holder. The collaborative and relational dynamics of social media challenge the very idea of individual consent, especially since users who agree to data collection may unknowingly disclose information about third parties, such as friends, family members, or followers who have not explicitly agreed to participate. Consequently, consent often becomes a formalized and opaque mechanism, better described as uninformed consent—users typically accept generalized terms of service that seem to assign ownership of content to them, while granting platforms broad rights of use and redistribution [54,58]. To address these issues, Nunan and Yenicioglu [57] suggest a participatory consent model—a continuous and relational process that restores users' agency in defining and monitoring how their data is used. As several scholars note, privacy expectations are deeply contextual [59]. For this reason, researchers have argued for situated, iterative, and participatory models of consent [60]. It is also important to note that informed consent faces challenges not only in big data scenarios but also in small data research, which tends to be more focused, qualitative, and interactive. In the digital environment, communication between researchers and participants is mediated by technological tools [51], making it harder to ensure that informed consent is genuinely understood. The direct, dialogic engagement typical in traditional research settings is often absent. In netnography, this separation is especially significant in studies conducted in semi-public or hybrid digital spaces—such as forums, closed groups, or social platforms—where users may not see themselves as participating in a "public sphere" [13]. In such cases, informed consent cannot be treated as just procedural; instead, it requires a situated reflection that considers users' privacy expectations and the nature of the communication within the observed context. The dynamic, continually changing nature of digital environments complicates ethics. Unlike classic research, consent cannot be treated as a single, stable event—digital data are enriched with metadata, reshaped, and interlinked, while users enter and exit platforms. In such conditions, informed

consent is better conceived as iterative and situated—e.g., via double, delayed, or implicit consent—and this is also the case in qualitative approaches like netnography [19].

Anonymity poses parallel challenges because it is entangled with identity. Curlew [61] shows how anonymous platforms foster "undisciplined performativity," enabling expression beyond legal identities and redefining norms, accountability, and responsibility. Anonymity is thus not merely technical but performative.

Digital data are intrinsically relational. Even without direct identifiers, cross-referencing datasets and mining metadata can enable re-identification [62]), and even anonymized datasets remain vulnerable to various forms of attack that can enable identities to be reconstructed [63,64]; Basso et al., 2016), while algorithmic profiling can infer sensitive attributes. Anonymous datasets may become identifiable when combined with geographic or temporal information, and persistent digital traces strain identity protection. Taking into account these aspects, anonymity should not be conceived as an absolute issue, but as a practice that is context-sensitive, to be negotiated on a case-by-case basis in digital social research [65,66].

In this perspective, research on anonymity as a socio-technical phenomenon [65] highlights that it arises from technologies, social practices, cultures, and public representations. Technically, tools such as VPNs and end-to-end encryption can shield identity, but they are dual-use. Socially, anonymity depends on how users perceive and employ these tools—often without full awareness of their actual protection or exposure.

For these reasons, ethical approaches to anonymity need to be sensitive to the socio-technical configurations of the digital environment, jointly accounting for technical infrastructures, user practices, cultural expectations, and platform design. The challenges associated with anonymity also extend to qualitative and observational research, including netnographic studies. In these studies, anonymization requires careful consideration of not only usernames, but also narrative details, screenshots, and modes of interaction that could potentially disclose the identities of the individuals under observation [19]. In this sense, some studies [67] propose strategies such as the use of pseudonyms, continuous negotiation of informed consent and collaboration with participants to balance confidentiality and data integrity. From this perspective, anonymization aims to become a flexible ethical process rather than a rigid, predetermined one.

Another key issue is confidentiality. In the digital context, this means not only securely storing data but also preventing it from being traceable or re-identifiable [23]. Online platforms, which are often used to store research data, do not always provide adequate protection. Even when data is encrypted or anonymized, traceability can pose a risk, especially when data is shared among researchers or stored on third-party servers, such as cloud services, which may be vulnerable to unauthorized access [60,68].

In digital social research, safeguarding confidentiality requires an integrated, socio-technical approach—align regulatory and ethical obligations (e.g., the GDPR and other supranational frameworks) with technical protections such as encryption, data obfuscation, and secure backup, and reinforce these with robust organizational practices and careful attention to informed consent and participant rights [69]. Furthermore, the protection of sensitive data also supports digital trust and the legitimacy of research practices [68].

A central challenge lies in the technical and infrastructural vulnerabilities of contemporary platforms. Much research data are hosted and processed by third-party services with proprietary architectures and opaque operations beyond researchers' control [58]. Reliance on these tools introduces risks that are not always visible or predictable, heightening data exposure.

For example, administering online questionnaires through external platforms typically stores participants' responses on remote servers subject to different jurisdictions and

regulatory regimes. In such cases, responsibility for protection is partially delegated to infrastructures that may not be fully auditable or accountable [23]. The ethical integrity of research data is thus compromised by opaque platform governance and by non-transparent data collection practices, both of which erode the trust-based relationship between researcher and participant [70].

Furthermore, in the current context of open science, tensions can arise between the principle of confidentiality and the need to publicly share research data [71]. For example, making collected data available through open data repositories can conflict with ethical obligations to protect participants, particularly when the data is potentially identifiable, originates from sensitive environments, or does not align with participants' perception of privacy and the technical visibility of the data.

Confidentiality is more than just a technical issue. It is also relational, reflecting the researcher's ethical responsibility to protect what participants share—whether intentionally, unintentionally, or unconsciously—as well as what is automatically and broadly generated within interconnected digital environments. Therefore, confidentiality should be regarded as a principle that combines secure infrastructural management with attention to the relational and contextual aspects of research, as well as the participatory possibilities that digital spaces provide [72]. In this context, ethics in digital social research cannot be a fixed set of rules, but an ongoing, contextual practice that involves continuous reflexivity, interdisciplinary dialog, and careful thinking about the social, technical, cultural, and political implications of knowledge production. Traditional principles—such as informed consent, anonymity, and confidentiality—need be redefined for modern socio-technical environments [70]. However, this redefinition does not represent a break with or replacement of traditional ethical frameworks; indeed, it is a process of continuous adaptation between human values and socio-technical infrastructures [73]. In other words, the ethical challenges of digital social research do not abandon the traditional principles of social research ethics, but rather recontextualize them to address emerging issues related to the role of algorithms, platform characteristics, and digital data [21]. Research ethics thus becomes an iterative and reflective practice that situatedly and flexibly incorporates the founding principles into socio-technical environments, giving shape to a contextual ethics of social data [70]. Such ethics are constructed through concrete cases, interdisciplinary dialog processes, and the continuous review of practices [60]. These considerations require the implementation of both institutional and operational countermeasures.

Ethical review processes and research ethics committees (IRBs), for example, are evolving towards adaptive frameworks capable of assessing socio-technical risks and the dynamic nature of digital data [23,74] (Townsend & Wallace, 2016; Metcalf & Crawford, 2016).

Conversely, principles such as privacy by differential privacy and advanced encryption technologies help to operationalize ethics in digital social research, activating forms of protection directly within data infrastructures [69].

Together, these perspectives converge towards a model of ethics by design, in which ethical principles become an integral part of both research governance and the technical architectures that support it [70]. Based on this perspective, a further priority concerns cultivating awareness of the digital infrastructures and algorithmic logics that mediate participation and data generation. Developing algorithmic awareness, i.e., the capacity to recognize where and how algorithms operate across digital contexts, supports more critical and responsible engagement, guiding users' navigation of content and interaction modalities [75–77]. Such awareness also equips both users and researchers to scrutinize how diverse actors deploy these technologies and to anticipate their broader implications for choice, participation, and the use of digital data.

5. Discussion

The paper focuses on people in digital social research, emphasizing their role in data generation, as well as the risks they face—often unknowingly participating in research—and the need to rethink established principles such as informed consent, anonymity, and confidentiality. Many specific challenges for digital social research stem from the new nature of digital data and the possibilities for collection and analysis. The motivation behind this paper was the recognition that, in digital social research, data are people—even when they appear as texts or traces—and that their involvement introduces innovative challenges due to the separation between data, people, and researchers, along with their increasing disembodiment. Some data are more directly linked to people, such as in netnography or social media research, where data are narratives focused on identity, personal issues, vulnerable populations, and sensitive topics. However, data not immediately linked to individuals can still impact lives in unexpected ways; for example, location coordinates can reveal people's movements or home locations. This prompts us to view digital social research as human-based rather than purely text-based. Since it involves humans, this type of research can cause harm—breaches of privacy, dataveillance, dependence, manipulation, deception, and discrimination are key challenges, driven by ambiguous public–private boundaries, non-neutral algorithms, algorithmic personalization, re-identification risks, and other digital dynamics. Harm also arises from difficulties in applying responsible research rules. Obtaining informed consent is challenging in digital contexts, especially in big data research, and anonymity and confidentiality are continually threatened by relationality and traceability, increasing the risk of re-identification.

We identify two main challenges facing digital social research. The first challenge lies in the risk of dehumanizing data under the previously discussed three-pronged separation. Re-humanizing data requires a practice of care toward information inseparable from people's lives. In digital social research, a care principle means centering participants' well-being: anticipating concerns and potential harms and protecting them from unintended consequences. Enthusiasm for abundant, storable, and repurposable data must be tempered by epistemic and ethical vigilance, understood as mutually entangled.

On the epistemic side, the nature of knowledge is limited by people's lack of intentionality and reflexivity in producing digital information, their lack of awareness of its research use, and the absence of dialog. This results in indirect ethical consequences related to research products because it could lead to unfaithful representations of people. These issues are in addition to the direct consequences of collecting private data, re-identifying anonymized data, discrimination in selecting information, or outcomes of research findings.

The second major risk spans digital social research perpetrating human rights violations, such as the right to self-representation; deciding which information is relevant (autonomy); and affecting equality (equal opportunities). To prevent these risks, social researchers must move beyond profiling logic that ignores identity, instead promoting a form of re-individualization against the de-individualization driven by algorithms. The focus for researchers is not just the data but the nuanced combination of individuals, context, and relationships that the data embodies—without which the information, as currently conceived in research, is not only unnatural but also meaningless, lacking interpretive tools for understanding its significance.

6. Limitations

The discussion on the implications of digital research for people is underdeveloped in the literature. From this perspective, this paper fills a gap. However, it is not without limitations.

First, it focuses on the risks for people and researchers in digital social research, thus sacrificing its potential to empower hidden populations, tackle sensitive topics, and so on. However, the potential of digital social research has been duly noted in many studies, alongside its risks. Hence, we decided to focus on the latter.

Second, it presents a general discussion of implications, which means it is not platform- and context-specific. Obviously, the types of data and risks may change according to platform affordances and specificities. This may be a direction for future research.

Third, it provides an exclusive theoretical discussion of the implications of digital social research for people. However, it may represent the first step towards designing an empirical study on how people perceive their online profiling, as well as their degree of awareness of data generation and their experience with violations.

7. Conclusions

Many concrete challenges for digital social research are connected to the different types of data and resulting possibilities for analysis. Ethical protocols and practices are focused on assumptions that are difficult to apply to digital social research, particularly regarding the data generated through research interactions (such as surveys, questionnaires, and interviews). Instead, digital traces are human-based found and transactional data, produced intentionally or unintentionally for purposes other than research, and sometimes as a product of other activities. By considering such data as representing humans, this paper focuses on the human impact of digital social research, stressing the importance of considering it human–subject research. This appears particularly important due to the continually contested boundaries of human–subject research and the diffused trend of considering digital research as not impacting people's lives, and so these aspects were exempted from review. This is vindicated by the abstraction of digital social research at different levels:

- In representing people through data which are partial and disembodied representations of identities.
- In interacting with people often through weak relationships or sometimes without even interacting.

Such abstraction makes standard research ethical protocols and their assumptions less applicable to the circumstances in which digital data are generated, stored, and analyzed.

The abstract subject changes the notions of the individual that we have been trained to adopt for several centuries. Digital traces are not about who you are but what you are like. Also, the privacy principle changes in front of this abstract subject. Privacy breaches are no longer related to the disclosure of personal information such as names, age, gender, etc. The risks we have identified may affect people without identifying their essential personality. Ethical principles need to be reframed according to the changing subject and based on novel notions of subjective personality. The question is no longer related to the disclosure of personal information, but to stripping the subject of their control over performative data.

The abstract links between researchers and participants reduce the sense of responsibility. However, privacy invasions, loss of autonomy, manipulation, deception, and discrimination increase concerns about responsibility and fairness. The challenge lies in detecting responsibility when harm occurs, preventing social research from reinforcing existing discrimination, and safeguarding privacy and autonomous decision-making, requiring cautious, context-specific approaches. As Quinton and Reynolds [34] argue, digital research demands a situated and reflexive ethical approach to develop reflexivity about choices and whether they will affect the outcome, how they will impact the outcome, and in which way people will seek to represent and reflexively and flexibly adapt to the context. Each project must carefully evaluate ethical risks, considering the context, data types, and

vulnerabilities involved. Although challenging, ethical digital social research requires the development of reflexivity in relation to data, decisions, and their potential impact on individuals to ensure our methods remain aligned with long-standing ethical principles.

In light of this discussion, it is possible to return to the main research question and the two secondary questions to summarize the results of the study.

Regarding the MRQ, which concerns the object of research in digital social research, it can be said that, in digital contexts, the subject of research no longer pertains to just the individual, but rather a socio-technical whole composed of people, their traces, profiles, and the algorithmic processes that describe and structure them, as well as elements that can have concrete effects on people's lives.

Returning specifically to RQ1, which concerns the types of risks to individuals, digital social research exposes individuals to a range of ethical and social issues, ranging from privacy violations and re-identification, to pervasive data surveillance and the consequent loss of autonomy, as well as to digital discrimination processes generated by distorted and opaque algorithms. These risks are amplified by the three-pronged separation between data, people, and researchers, which tends to blur responsibilities and weaken awareness of the consequences of research.

Finally, with regard to RQ2, which questioned how research ethics should adapt to digital contexts, the latest developments indicate the need for a situated and continuous approach. This involves adopting forms of iterative and participatory consent, using contextual anonymization and conceiving of confidentiality not only from a technical point of view (realized, for example, in encryption systems, secure storage systems, and other systems.) but also based on the principles of relational trust between researchers and research subjects. Added to this are fundamental processes of algorithmic awareness and transparency in data infrastructure and information collection and use processes, ensuring that digital social research is grounded in responsibility, fairness, and the protection of people's rights.

Author Contributions: Conceptualization, F.R.L., A.D.P., and M.C.C.; Methodology, F.R.L., A.D.P., and M.C.C.; Resources, F.R.L., A.D.P., and M.C.C.; Writing—Original Draft, F.R.L., A.D.P., and M.C.C.; Writing—Review and Editing, F.R.L., A.D.P., and M.C.C.; Supervision, A.D.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Delli Paoli, A.; Masullo, G. Digital social research: Topics and methods. *Ital. Sociol. Rev.* **2022**, *12*, 617–633. [CrossRef]
2. Vassilakopoulou, P.; Hustad, E. Bridging digital divides: A literature review and research agenda. *Inf. Syst. Front.* **2023**, *25*, 955–969. [CrossRef]
3. Japec, L.; Kreuter, F.; Berg, M.; Biemer, P.; Decker, P.; Lampe, C.; Usher, A. Big data in survey research: AAPOR task force report. *Public Opin. Q.* **2015**, *79*, 839–880. [CrossRef]
4. Royakkers, L.; Timmer, J.; Kool, L.; van Est, R. Societal and ethical issues of digitization. *Ethics Inf. Technol.* **2018**, *20*, 127–142. [CrossRef]
5. Olteanu, A.; Castillo, C.; Diaz, F.; Kıcıman, E. Social data: Biases, methodological pitfalls, and ethical boundaries. *Front. Big Data* **2019**, *2*, 13. [CrossRef]
6. Amaturo, E.; Aragona, B. Methods for big data in social sciences. *Math. Popul. Stud.* **2019**, *26*, 65–68. [CrossRef]
7. Lupton, D. Understanding the human machine. *IEEE Technol. Soc. Mag.* **2013**, *32*, 25–30. [CrossRef]

8. Kambil, A. What is your Web 5.0 strategy? *J. Bus. Strategy* **2008**, *29*, 56–58. [CrossRef]
9. Cambria, E. Affective computing and sentiment analysis. *IEEE Intell. Syst.* **2016**, *31*, 102–107. [CrossRef]
10. Rudder, C. *Dataclysm: Love, Sex, Race, and Identity–What Our Online Lives Tell Us about Our Offline Selves*; Broadway Books: New York, NY, USA, 2015.
11. Rose, N. The politics of life itself. *Theory Cult. Soc.* **2001**, *18*, 1–30. [CrossRef]
12. Barry, L. The quantified self and the digital making of the subject. In *The Digital Age and Its Discontents: Critical Reflections in Education*; Stocchetti, M., Ed.; Helsinki University Press: Helsinki, Finland, 2020; pp. 95–110. [CrossRef]
13. Delli Paoli, A. *La Netnografia Nella Ricerca Sociale*; FrancoAngeli: Milano, Italy, 2025.
14. Lupton, D. Not the real me?: Social Imaginaries of Personal Data Profiling. *Cult. Sociol.* **2021**, *15*, 3–21. [CrossRef]
15. Goriunova, O. The Digital Subject: People as Data as Persons. *Theory Cult. Soc.* **2019**, *36*, 125–145. [CrossRef]
16. Goffman, E. *The Presentation of Self in Everyday Life*; Doubleday: New York, NY, USA, 1959.
17. Ashford, C. Queer theory, cyber-ethnographies and researching online sex environments. *Inf. Commun. Technol. Law* **2009**, *18*, 297–314. [CrossRef]
18. Tiidenberg, K. Ethics in digital research. In *The SAGE Handbook of Qualitative Data Collection*; Flick, U., Ed.; Sage: London, UK, 2018; pp. 466–481.
19. Delli Paoli, A. On the ethics of social research in netnography. *Lab's Q.* **2025**, *27*, 1–26.
20. Markham, A.N.; Tiidenberg, K.; Herman, A. Ethics and methods: Doing ethics in the era of big data research—Introduction. *Soc. Media + Soc.* **2018**, *4*, 2056305118784502. [CrossRef]
21. Markham, A.N. Afterword: Ethics as Impact—Moving from Error-Avoidance and Concept-Driven Models to a Future-Oriented Approach. *Soc. Media + Soc.* **2018**, *4*, 2056305118784504. [CrossRef]
22. Dieterle, B. People as data? Developing an ethical framework for feminist digital research. *Comput. Compos.* **2021**, *59*, 102630. [CrossRef]
23. Metcalf, J.; Crawford, K. Where are human subjects in big data research? The emerging ethics divide. *Big Data Soc.* **2016**, *3*, 2053951716650211. [CrossRef]
24. Zook, M.; Barocas, S.; Boyd, D.; Crawford, K.; Keller, E.; Gangadharan, S.P.; Pasquale, F. Ten simple rules for responsible big data research. *PLoS Comput. Biol.* **2017**, *13*, e1005399. [CrossRef]
25. Clarke, R.; Greenleaf, G. Dataveillance regulation: A research framework. *J. Law Inf. Sci.* **2017**, *25*, 104. [CrossRef]
26. Büchi, M.; Festic, N.; Latzer, M. The chilling effects of digital dataveillance: A theoretical model and an empirical research agenda. *Big Data Soc.* **2022**, *9*, 20539517211065368. [CrossRef]
27. Müller, L. Domesticating artificial intelligence. *Moral Philos. Politics* **2022**, *9*, 219–237. [CrossRef]
28. Kozinets, R.V.; Gambetti, R. *Netnography Unlimited*; Routledge: London, UK, 2021. [CrossRef]
29. Marres, N.; Weltevrede, E. Scraping the social? Issues in live social research. *J. Cult. Econ.* **2013**, *6*, 313–335. [CrossRef]
30. Zuo, Z.; Watson, M.; Budgen, D.; Hall, R.; Kennelly, C.; Al Moubayed, N. Data anonymization for pervasive health care: Systematic literature mapping study. *JMIR Med. Inform.* **2021**, *9*, e29871. [CrossRef] [PubMed]
31. Campedelli, M.; Vesan, P. Welfare digitalizzato, welfare digitale e i nuovi rischi sociali digitali: Un'introduzione. *Politiche Soc./Soc. Policies* **2023**, *2*, 169–192.
32. Fainmesser, I.P.; Galeotti, A.; Momot, R. Digital privacy. *Manag. Sci.* **2023**, *69*, 3157–3173. [CrossRef]
33. Soumelidou, A.; Papaioannou, T. An information privacy competency model for online consumers. In *International Conference on Research Challenges in Information Science*; Springer: Cham, Switzerland, 2023; pp. 593–602.
34. Quinton, S.; Reynolds, N. The changing roles of researchers and participants in digital and social media research: Ethics challenges and forward directions. In *The Ethics of Online Research*; Woodfield, K., Ed.; Emerald Publishing Limited: Leeds, UK, 2017; pp. 53–78. [CrossRef]
35. Schneier, B. *Data and Goliath: The hidden Battles to Collect Your Data and Control Your World*; W. W. Norton: New York, NY, USA, 2015.
36. Zuboff, S. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*; Public Affairs: New York, NY, USA, 2019.
37. Reiman, J.H. Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Comput. High Technol. Law J.* **1995**, *11*, 27–44.
38. Clarke, R. Information technology and dataveillance. *Commun. ACM* **1988**, *31*, 498–512. [CrossRef]
39. Lupton, D.; Michael, M. Depends on who's got the data: Public understandings of personal digital dataveillance. *Surveill. Soc.* **2017**, *15*, 254–268. [CrossRef]
40. Rubinstein, I.S.; Lee, R.D.; Schwartz, P.M. Data mining and internet profiling: Emerging regulatory and technological approaches. *Univ. Chic. Law Rev.* **2008**, *75*, 261.
41. Favaretto, M.; De Clercq, E.; Elger, B.S. Big data and discrimination: Perils, promises and solutions. A systematic review. *J. Big Data* **2019**, *6*, 12. [CrossRef]

42. Criado, N.; Such, J.M. *Digital Discrimination in Algorithmic Regulation*; Oxford University Press: Oxford, UK, 2019.
43. Angwin, J.; Larson, J.; Mattu, S.; Kirchner, L. *Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks*; ProPublica: New York, NY, USA, 2016; Available online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing (accessed on 1 November 2025).
44. Spitale, G.; Biller-Andorno, N.; Germani, F. AI model GPT-3 (dis)informs us better than humans. *Sci. Adv.* **2023**, *9*, eadh1850. [CrossRef]
45. Pariser, E. *The Filter Bubble: What the Internet is Hiding from You*; Penguin: London, UK, 2011.
46. Dahlgren, P.M. A critical review of filter bubbles and a comparison with selective exposure. *Nord. Rev.* **2021**, *42*, 15–33. [CrossRef]
47. Palazzani, L. *Tecnologie Dell'informazione e Intelligenza Artificiale: Sfide Etiche al Diritto*; Edizioni Studium: Roma, Italy, 2020.
48. Lombi, L. La ricerca sociale al tempo dei big data: Sfide e prospettive. *Studi Sociol.* **2015**, *2*, 215–227.
49. Mittelstadt, B.D.; Allo, P.; Taddeo, M.; Wachter, S.; Floridi, L. The ethics of algorithms: Mapping the debate. *Big Data Soc.* **2016**, *3*, 2053951716679679. [CrossRef]
50. Hennell, K.; Limmer, M.; Piacentini, M. Ethical dilemmas using social media in qualitative social research: A case study of online participant observation. *Sociol. Res. Online* **2020**, *25*, 473–489. [CrossRef]
51. Halford, S. The ethical disruptions of social media data: Tales from the field. In *The Ethics of Online Research*; Woodfield, K., Ed.; Emerald Publishing Limited: Leeds, UK, 2017; pp. 13–25.
52. Geier, C.; Kim, H.; Lee, J. Informed consent for online research—Is anybody reading? Assessing comprehension and individual differences in reading consent forms. *J. Empir. Res. Hum. Res. Ethics* **2021**, *16*, 25. [CrossRef] [PubMed]
53. Sloan, L.; Jessop, C.; Al Baghal, T.; Williams, M. Linking survey and Twitter data: Informed consent, disclosure, security, and archiving. *J. Empir. Res. Hum. Res. Ethics* **2020**, *15*, 63–76. [CrossRef]
54. Clark, B.; McGrath, C.; McMillan, C.; McDonald, P. Advancing the ethical use of digital data in human research: Challenges and strategies to promote ethical practice. *J. Empir. Res. Hum. Res. Ethics* **2019**, *14*, 433–445. [CrossRef]
55. Nycyk, M. Ethical use of informant internet data: Scholarly concerns and conflicts. *J. Digit. Soc. Res.* **2022**, *4*, 1–22. [CrossRef]
56. Gupta, S. Ethical issues in designing internet-based research: Recommendations for good practice. *J. Res. Pract.* **2017**, *13*, D1.
57. Nunan, D.; Yenicioglu, B. Informed, uninformed and participative consent in social media research. *Int. J. Mark. Res.* **2013**, *55*, 791–808. [CrossRef]
58. Boyd, D.; Crawford, K. Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. *Inf. Commun. Soc.* **2012**, *15*, 662–679. [CrossRef]
59. Nissenbaum, H. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*; Stanford University Press: Stanford, CA, USA, 2010.
60. Markham, A.; Buchanan, E. Ethical decision-making and internet research. *Assoc. Internet Res.* **2012**. Available online: http://aoir.org/reports/ethics2.pdf (accessed on 1 October 2025).
61. Curlew, A. Undisciplined performativity: Improvised subjectivity and anonymity in digital space. *Soc. Media + Soc.* **2019**, *5*, 2056305119829843. [CrossRef]
62. Narayanan, A.; Shmatikov, V. Robust de-anonymization of large sparse datasets. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (SP 2008), Oakland, CA, USA, 18–22 May 2008; IEEE: New York, NY, USA, 2008; pp. 111–125.
63. Zimmer, M. But the data is already public: On the ethics of research in Facebook. *Ethics Inf. Technol.* **2010**, *12*, 313–325. [CrossRef]
64. Basso, T.; Matsunaga, R.; Moraes, R.; Antunes, N. Challenges on anonymity, privacy, and big data. In *2016 Seventh Latin-American Symposium on Dependable Computing (LADC)*; IEEE: New York, NY, USA, 2016; pp. 164–171.
65. Sardá, T.; Natale, S.; Sotirakopoulos, N.; Monaghan, M. Understanding online anonymity. *Media Cult. Soc.* **2019**, *41*, 557–564. [CrossRef]
66. Marwick, A.; Boyd, D. It's complicated. *Qual. Res. Psychol.* **2014**, *12*, 125–137.
67. Saunders, B.; Kitzinger, J.; Kitzinger, C. Participant anonymity in the internet age: From theory to practice. *Qual. Res. Psychol.* **2015**, *12*, 125–137. [CrossRef]
68. Livraga, G.; Viviani, M. Data confidentiality and information credibility in online ecosystems. In Proceedings of the 11th International Conference on Management of Digital Ecosystems, Limassol, Cyprus, 12–14 November 2019; ACM: New York, NY, USA, 2019; pp. 191–198.
69. Floridi, L.; Taddeo, M. What is data ethics? *Philos. Trans. R. Soc. A Math. Phys. Eng. Sci.* **2016**, *374*, 20160360. [CrossRef] [PubMed]
70. Williams, M.L.; Burnap, P.; Sloan, L. Towards an ethical framework for publishing Twitter data in social research: Taking into account users' views, online context and algorithmic estimation. *Sociology* **2017**, *51*, 1149–1168. [CrossRef] [PubMed]
71. Pasquetto, I.V.; Randles, B.M.; Borgman, C.L. On the reuse of scientific data. *Data Sci. J.* **2017**, *16*, 1–9. [CrossRef]
72. Indriasari, D.T.; Karman, K. Privacy, confidentiality, and data protection: Ethical considerations in the use of the internet. *Int. J. Islam. Educ. Res. Multicult. (IJIERM)* **2023**, *5*, 431–450. [CrossRef]
73. Floridi, L. *The Ethics of Information*; Oxford University Press: Oxford, UK, 2013.
74. Townsend, L.; Wallace, C. *Social Media Research: A Guide to Ethics*; University of Aberdeen: Aberdeen, UK, 2016.

75. Felaco, C. Researching algorithm awareness: Methodological approaches to investigate how people perceive, know, and interact with algorithms. *Math. Popul. Stud.* **2024**, *31*, 267–288. [CrossRef]
76. Koenig, A. The algorithms know me and I know them: Using student journals to uncover algorithmic literacy awareness. *Comput. Compos.* **2020**, *58*, 102611. [CrossRef]
77. Dinev, T.; Hu, Q. The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *J. Assoc. Inf. Syst.* **2007**, *8*, 23. [CrossRef]