Digital Stewardship

Digital self-determination

https://en.m.wikipedia.org/wiki/Digital_self-determination

Digital self-determination is a multidisciplinary concept derived from the legal concept of self-determination and applied to the digital sphere, to address the unique challenges to individual and collective agency and autonomy arising with increasing digitalization of many aspects of society and daily life.

There is no philosophically or legally agreed-upon concept of digital self-determination yet. Broadly speaking, the term describes the attempt to comprehensively project the pattern of human self-determination (as first explored in disciplines like philosophy and psychology, and in the law) into the digital age.

The concept has been included in an official document for the first time by ARCEP, the French Telecoms Regulator, in a section of its 2021 Report on the State of the Internet,[1] exploring the work on "Network Self-determination"[2] conducted by Professor Luca Belli.

The concept of self-determination relates to concepts of subjectivity, dignity, and autonomy in classic central-European philosophy and derived from Immanuel Kant's conception of freedom. Self-determination presupposes that human beings are entities capable of reason and responsibility for their own rationally chosen and justified actions (autonomy), and ought to be treated accordingly. In formulating his categorical imperative (kategorischer Imperativ), Kant suggested that humans, as a condition of their autonomy, must never be treated as a means to an end but as an end in itself. The pattern of self-determination similarly aims at enabling autonomous human beings to create, choose and pursue their own identity, action, and life choices without undue interference.

The increasing digitization of most aspects of society poses new challenges for the concept and realization of self-determination.[7] While the digital sphere has ushered in innovation and opened up new opportunities for self-expression and communication for individuals across the globe, its reach and benefits have not been evenly distributed, oftentimes deepening existing inequalities and power structures, commonly referred to as a digital divide. Moreover, the digital transformation has enabled, oftentimes unbeknownst to individuals, the mass collection, analysis, and harvesting of personal data by private companies and governments to infer individuals' information and preferences (e.g., by tracking browsing and shopping history), influence opinions and behavior (e.g., through filter bubbles and targeted advertisements), and/or to make decisions about them (e.g., approving or not a loan or employment application), thus posing new threats to

individuals' privacy and autonomy.[8]

Although the definition of digital self-determination is still evolving, the term has been used to address humans' capacity (or lack thereof) to exercise self-determination in their existence in and usage of digital media, spaces, networks, and technologies, with the protection of the potential for human flourishing in the digital world as one of the chief concerns.[9]

Data Sovereignty

Data sovereignty is the concept that data is subject to the laws and regulations of the country or region where it was generated or is stored. It essentially means that a country has the authority to govern the data within its borders, including how it's stored, processed, and protected.

https://en.m.wikipedia.org/wiki/Data_sovereignty

Data sovereignty is the idea that data are subject to the laws and governing structures of the nation where they are collected. In other words, a country is able to control and access the data that is generated in its territories.[1] An example of a nation's data sovereignty policy would be Australia's Privacy Policy guidelines, also known as APP. [2] The APP contains 13 principles for how all personal or organizational data in Australia is meant to be kept.[2] For many countries, the issue of data sovereignty is presented as an issue of national security with concerns over being able to protect citizens' personal data.[1] Data can be used to help improve medical care, reinforce national security as well as have a positive impact on many economic and social infrastructures but may also be used for identity theft and other data related attacks.[1]

The concept of data sovereignty is closely linked with data security, cloud computing, network sovereignty, and technological sovereignty. Unlike technological sovereignty, which is vaguely defined and can be used as an umbrella term in policymaking,[3] data sovereignty is specifically concerned with questions surrounding the data itself.[4] The issue of managing data sovereignty can be considered more complex when introducing the idea of cloud computing, where data can be accessed globally; meaning organizations and companies must comply with multiple nations data laws.[5] Data sovereignty is also associated with data localization, the requirement that data be stored within a specified region, and data residency, the actual location in which the data is stored, such as cloud servers.[1]

Data sovereignty as the idea that data is subject to the laws and governance structures within one nation, is usually discussed in one of two ways: in relation to Indigenous groups and Indigenous autonomy from post-colonial states, or in relation to transnational data flow.[6] With the rise of cloud computing, many countries have passed various laws around the control and storage of data, which all reflect measures of data sovereignty.[4] More than 100 countries have some form of data sovereignty laws in place.[7] With

self-sovereign identity (SSI), the individual identity holders can fully create and control their credentials, although a nation can still issue a digital identity in that paradigm.[8]

https://en.m.wikipedia.org/wiki/Data_sovereignty_(data_management)

Data sovereignty is the ability of a legal person or an organisation to control the conditions that data is shared under, and how that shared data is used, as if it were an economic asset.[1][2] It can apply to both primary data and secondary data derived from data, or metadata.[3] In order to use restricted data, data consumers must accept the conditions that it is provided under.[4] In turn, the legal persons sharing data must trust other entities with it. Trust can be supported through the use of a suitable secure information system (such as a data space) which identifies, authenticates, and certifies users.[5]

The data sovereignty of individual legal persons can conflict with national data sovereignty.[6] Currently, a natural person does not have a statutory right to exclusively control how their data is shared and used. However, they can make it part of a contract, and offer it as payment.[7] The most common method for a legal person to impose its data sovereignty is through contract law.[8] Such a contract includes the terms of use, access and control policies, commercial conditions and jurisdiction.[3]

The use of cloud services can make it difficult to determine where data is physically located and which law applies

A common criticism of data sovereignty brought forward by corporate actors is that it impedes and has the potential to destroy processes in cloud computing.[30] Since cloud storage might be dispersed and disseminated in a variety of locations at any given time, it is argued that governance of cloud computing is difficult under data sovereignty laws.[30] For example, data held in the cloud may be illegal in some jurisdictions but legal in others.[4]The concept of a sovereign cloud is proposed as a solution to address this challenge.[31][32]

Data governance

Scholar Shoshana Zuboff popularized the term surveillance capitalism to refer to the private sector's commodification of users' personal data for profit (e.g. via targeted advertising), leading to increased vulnerability to surveillance and exploitation. Surveillance capitalism relies on centralized data management models wherein private companies retain ownership and control over the users' data. To guard against the challenges to individuals' privacy and self-determination, various alternative data governance models have been recently proposed around the world, including trusts,[32] commons,[33] cooperative,[34] collaboratives,[35] fiduciaries,[36] and "pods".[37] These models have some overlap and share a common mission to give more control to individuals over their data and thus address the current power imbalances between data holders and data subjects.[38]

Freedom & Privacy

Intellectual freedom & censorship

Censorship online can be carried out (to varying degrees) by actors including totalitarian governments, network administrators, and service providers. These efforts to control communication and restrict access to information will always be incompatible with the human right to Freedom of Expression.5

Censorship on corporate platforms is increasingly common, as platforms like Twitter and Facebook give in to public demand, market pressures, and pressures from government agencies. Government pressures can be covert requests to businesses, such as the White House requesting the takedown of a provocative YouTube video, or overt, such as the Chinese government requiring companies to adhere to a strict regime of censorship.

People concerned with the threat of censorship can use technologies like Tor to circumvent it, and support censorship-resistant communication platforms like Matrix, which doesn't have a centralized account authority that can close accounts arbitrarily.

You must always consider the risks of trying to bypass censorship, the potential consequences, and how sophisticated your adversary may be. You should be cautious with your software selection, and have a backup plan in case you are caught.

Representation of diverse realities and viewpoints

Internet activist Eli Pariser coined the term filter bubble to refer to the reduced availability of divergent opinions and realities that we encounter online as a consequence of personalization algorithms like personalized search and recommendation systems.[30] Filter bubbles have been suggested to facilitate a warped understanding of others' points of view and the world. Ensuring a wide representation of diverse realities on digital platforms could be a way of increasing exposure to conflicting viewpoints and avoiding intellectual isolation into informational bubbles

Personal privacy

A common counter-argument to pro-privacy movements is the notion that one doesn't need privacy if they have **"nothing to hide."** This is a dangerous misconception, because it creates a sense that people who demand privacy must be deviant, criminal, or wrong.

You shouldn't confuse privacy with secrecy. We know what happens in the bathroom, but you still close the door. That's because you want privacy, not secrecy. There are always certain facts about us—say, personal health information, or sexual behavior—that we wouldn't want the whole world to know, and that's okay. The need for privacy is legitimate, and that's what makes us human. Privacy

is about empowering your rights over your own information, not about hiding secrets.

Take cookie consent forms, for example. You may encounter these dozens of times per day on the various websites you visit, with a nice array of checkboxes and sliders which allow you to "curate" your preferences to exactly fit your needs. In the end, we just hit the "I Agree" button, because we just want to read the article or make a purchase. Nobody wants to complete a personal privacy audit on every single website they visit. This is an exercise in choice architecture, designed to make you take the easy route out instead of delving into a maze of configuration options that don't need to exist in the first place.

Control over your privacy inside most apps is an illusion. It's a shiny dashboard with all sorts of choices you can make about your data, but rarely the choices you're looking for, like "only use my data to help me." This type of control is meant to make you feel guilty about your choices, that you "had the choice" to make the apps you use more private, and you chose not to.

Privacy is something we need to have baked into the software and services we use by default, you can't bend most apps into being private on your own.

Corporate surveillance

For many people, tracking and surveillance by private corporations is a growing concern. Pervasive ad networks, such as those operated by Google and Facebook, span the internet far beyond just the sites they control, tracking your actions along the way.

Additionally, even companies outside the *AdTech* or tracking industry can share your information with data brokers (such as Cambridge Analytica, Experian, or Datalogix) or other parties. You can't automatically assume your data is safe just because the service you're using doesn't fall within the typical AdTech or tracking business model.

Technological Stewardship

and Responsible Innovation

The call for responsible innovation is a call to address and account for technology’s short- and long-term impacts within social, political, environmental, and cultural domains.

Technological stewardship stands as the corollary of this mindset: a commitment to anticipate and mitigate technology’s potential for disruption and especially harm and to guide innovation toward beneficial ends.

Adopted from the domain of engineering ethics, where it “involves taking a value sensitive approach to embedding ethics, sustainability, and EDI (equity, diversity, and inclusivity) principles

into the practice and culture of engineering" [3, p. 34], technological stewardship belongs to any who would take up the mantle.

To be a technological steward means to be committed to an ethos of *care*: to understanding the systematic impacts of innovation and its philosophical dimensions, and to cultivating the capacity to apply this knowledge to drive development into new realms of humane engineering and design. To be a steward is to see care as the foundation of one's professional identity and not as an add-on or bonus. Technological stewardship is therefore about an optimistic turn toward the future of more responsible innovation—about recognizing the possibility for technology to transform culture and civilization and to steer away from the maelstrom of unfettered innovation.

Dialogue and collaboration across diverse perspectives is essential for developing actionable technological solutions that attend in responsible ways to the evolving needs of society.

Human-centered design of user interfaces and experiences

Scholars have coined the term attention economy to refer to the treatment of human attention as a scarce commodity in the context of ever-increasing amounts of information and products. In this view, the increasing competition for users' limited attention, especially when relying on advertising revenue models, creates a pressing goal for digital platforms to get as many people as possible to spend as much time and attention as possible using their product or service. In their quest for users' scarce attention, these platforms would be incentivized to exploit users' cognitive and emotional weaknesses, for example via constant notifications, dark patterns, forced multitasking, social comparison, and incendiary content.[8] Advocates of human-centered design in technology (or humane technology) propose that technology should refrain from such 'brain-hacking' practices, and instead should support users' agency over their time and attention as well as their overall wellbeing.[31]

Digital literacy

Digital literacy and media literacy have been proposed as necessary for individuals to acquire the knowledge and skills to use digital tools as well as to critically assess the content they encounter online, create their own content, and understand the features and implications of the digital technology used on them as well as the technology they consciously and willingly engage with.[28] In addition to basic digital navigation skills and critical consumption of information, definitions of digital literacy have been extended to include an awareness of existing alternatives to the digital platforms and services used, understanding how personal data is handled, awareness of rights and existing legal protections, and of measures to independently protect one's security and privacy online (e.g., the adoption of obfuscation techniques as a way of evading and protesting digital surveillance[29]).

Access to digital infrastructure and tools

Bridging the various forms of existing digital divides and providing equitable and fair access to digital technologies and the internet has been proposed as crucial to ensure that all individuals are able to benefit from the digital age, including access to information, services, and advancement opportunities.[24][25]

In this sense, the concept of Digital Self-determination overlaps with the concept of "Network Self-determination"[26] as it emphases that groups of unconnected and scarcely connected individuals can regain control over digital infrastructures, by building them and shaping the governance framework that will organise them as a common good.[27] As such, Belli stresses that network self-determination leads to several positive externalities for the affected communities, preserving the Internet as an open, distributed, interoperable and generative network of networks.[2]

Revision #6
Created 19 May 2025 20:54:55 by metaphorraccoon
Updated 9 June 2025 05:27:15 by metaphorraccoon