REPORT SECTION

Neutral but Not Innocent:

Data, Power and the Public Good

Ravale Mohydin

TRT WORLD research centre

The Rise of Data as a Political and Ethical Force

In the datafied world we inhabit, information has emerged as the foundation layer for governance, economic activity, healthcare, education and a lot more. With the proliferation of sensors, algorithms, and connected devices, the capacity to collect, process, and apply data at scale has increased dramatically. This shift has triggered profound ethical debates about surveillance, bias and manipulation, igniting fears that too much power is being ceded to data itself.

This discussion centres around the assertion that such concerns, while valid, often misplace the locus of ethical responsibility. Data is not inherently good or bad and can be considered to be a neutral resource. Its ethical valence emerges from how it is collected, structured, and applied, specifically by whom, under what conditions and to what ends. This position is explored by examining global examples where data has either empowered societies or been used to reinforce inequality and control, as well as interrogating the conditions under which its neutrality is compromised. A "devil's advocate" lens is adopted to explore the limits of data neutrality: Can any dataset be truly objective? Can infrastructure built on inherently biased social systems ever be considered neutral in impact? These questions are evaluated through multiple lenses, including algorithmic design, data governance, power asymmetries, and public accountability.

To transition from theoretical framing to applied contexts, this section presents a series of international case examples illustrating how data systems can both serve the public good and reinforce systemic control. The discussion includes examples of successful public-good-oriented data systems, including Türkiye's e-government platform, and calls for data ethics frameworks rooted in transparency, human rights and inclusivity. The paper ultimately argues that data must be governed, and not feared, for it to effectively serve the public good.

The Emergence of Data as Political and Ethical Power

Data metrics and scores appear to shape eligibility, risk and reputation in today's world. As this dynamic deepens, it invites questions such as whether the danger is rooted in data's sheer volume or its unaccountable deployment. The past two decades have witnessed a phenomenal transformation in how societies produce, consume, and rely on information. It is not merely a byproduct of internet activity but has become central to how governments govern, markets function, and people live. Information is the oil of the 21st century, the lifeblood of the digital economy and a mirror of our collective behaviour. However, this increasing power has raised an existential question. Are we witnessing the beginning of an era in which algorithmic determination, predictive analysis, and behavioural nudging quietly but compellingly drive outcomes in disparate realms such as criminal justice and marketing?

It then becomes pertinent to ask: What sort of "rule" does data ever have? Agency vested in the data itself or in the actors who handle it? These are not theoretical questions. They are political, economic, and profoundly ethical. Drawing on Michel Foucault's notion of power/knowledge, we can understand data not as a neutral input but as a medium through which power circulates (Foucault, 1980). In this view, data production and interpretation are never outside the sphere of governance, for they shape and are shaped by institutional agendas. Nancy Fraser's theory of "participatory parity" (Fraser, 2003, p.7) similarly offers a lens to critique data systems that claim neutrality but reproduce structural exclusions, particularly when access to data governance is restricted to elite or technocratic actors.

This analysis argues that data does not govern in any independent capacity. It is an amoral instrument, a tool offering much potential but no internal motive or moral compass. Data ethics come strictly from its utilisation and setting. A geospatial coordinate database can be applied to provide assistance in the case of a natural disaster or apply drone surveillance on a political activist. The data set remains unchanged; the morality is in the application. Nevertheless, neutrality is a tenuous and contested status. Even if raw data is neutral, its interpretation, collection, and use are always mediated by human judgment and institutional incentives. In this regard, neutrality should be considered a default, one that will need to be maintained through diligent stewardship rather than assumed.



(Muhammed Selim Korkutata - Anadolu Agency)

The Devil's Advocate: Is True Neutrality Even Possible?

What is meant by the statement "data is neutral"? To say data is neutral is to say it has no moral valence of its own. This view disconnects data as input, a collection of facts, signals, or observations, from decisions or actions taken based on the input. It is a rule long taken for granted in information science and theory: that a fact by itself is neither immoral nor moral. Consider rainfall data collected over a decade. Governments may use these to design flood defences or by agricultural firms to design planting cycles. Their collection is not in itself biased toward one actor or another. It is their interpretation and use i.e. what models they inform and what decisions they ratify, that introduce moral deliberations. This neutrality is analytically helpful. It has the effect of depersonalising information and directing critical scrutiny where it belongs: power relations, intention, and responsibility. It also works against alarmist discourses that view information as inherently intrusive or threatening.

However, critics quickly counter that data is never collected in a void. Choices about what to measure, how to categorise it, and what not to include are more likely than not to be socially, politically or economically driven. Even the idea of "raw data" is a myth: all data is cooked by the processes that create and present it (Gitelman & Jackson, 2013, p.2), which leads to a paradox. Data may appear neutral, but its use is shaped by context, requiring strong institutions to construct and enforce genuine neutrality through representation, regulation and public accountability.

Even if we allow for the theoretical neutrality of data, can it ever be neutral in practice? Playing the devil's advocate, not to disprove neutrality outright but to challenge its practical robustness can be enlightening in this case. To begin with, data is always construed by and for the collector's purpose. Variable definitions, choices, and sources are value-laden. Consider crime statistics. What constitutes a crime? Which neighbourhoods are more intensively patrolled? These delimit the dataset and, thereby, the algorithms trained upon it. Secondly, asymmetries of power shape data infrastructure (Milan & Treré, 2024). Billions-strong platforms have enormous power over what kinds of data are gathered and how they are leveraged. A nominally value-neutral dataset of user behaviour is translated into manipulative recommendation algorithms, ad targeting, or surveillance systems without users' knowledge or consent. Third, epistemic injustice is normally a result of groups being systematically excluded or misrepresented in data. Indigenous people, for example, regularly fall between the gaps of census and health data gathering. Their lack of visibility in data may lead them to be excluded from policy or resource distribution.

Therefore, neutrality is a norm, not an empirical fact. It's worth delineating an ethical ideal: that information should not be the preserve of the powerful, that it should be listened to with attention, and that its applications should be queried. Thus, defenders and advocates of data neutrality must be cautious, for neutrality is not a defence against criticism. It is an ethical obligation to protect the boundary between tool and weapon, of which data can be both.

When Data Empowers and Harms

For all its dangers, data, when properly governed, can significantly impact human experiences globally. Examples abound worldwide. The first is Estonia's system of e-governance, which enables individuals to vote, view medical records, and digitally sign documents but still retain ownership of the data (Republic of Estonia e-Governance Academy, 2023). The access to one's personal data is monitored and viewable by the citizen, thus providing an open loop of accountability. Another example is Türkiye's e-Devlet portal, which has simplified access to hundreds of state services, ranging from health coverage to report cards, for all citizens and residents (Republic of Türkiye Digital Transformation Office, n.d.; AFAD, n.d.). Coupled with the seismic data systems that AFAD maintains, Türkiye leveraged data to cut red tape and respond more efficiently to earthquakes. These examples illustrate how data infrastructures when grounded in public interest regimes, can establish trust, lower costs, and save lives. Across the Global South, from Nairobi to Bogotá, cities are developing open data portals on transport, waste, and crime, which are enabling civic tech start-ups to enhance the governance of cities. It has become abundantly clear that data, if made available, anonymised, and properly structured, is a public good.

Nevertheless, information can become perilous in the absence of strong governance because its application lacks accountability. A well-known example is the Cambridge Analytica debacle. In 2018, it was discovered that political consulting firm Cambridge Analytica had harvested millions of Facebook users' personal data without their consent. This data was used to disseminate microtargeted political ads, possibly swaying the 2016 American presidential election (Rosenberg, Confessore & Cadwalladr, 2018). In this instance, data was used to exploit psychological vulnerabilities, not through fabricated data, but through the illegal use of real data, to the alleged detriment of democracy.

Another example is China's social credit and surveillance system, which pulls data from banks, public records, and social media to give citizens a score (Botsman, 2017). A low score can result in limits on employment, travel, or even attendance at school. The facts are accurate, but the moral question is a centralised punitive application with minimal provision for appeal. An example of a more systemic misuse of data is predictive policing in the United States, which has been guided historically by biased data and has led to the over-policing of communities of colour (Benbouzid, 2019). Facial recognition technology has inaccurately identified Black people at a disproportionately higher rate, leading to wrongful arrests (Johnson & Johnson, 2023).

However, the deadliest example of data misuse is that of the Israeli military reportedly employing an artificial intelligence (AI) system known as "Where's Daddy?" during its operations in Gaza. This system is set up to track the movements of individuals who have been singled out as targets and, more particularly, to determine when targets are present in family households (Abraham, 2024). Strikes are timed to take place when targets are in their residences, which has the effect of resulting in civilian casualties, including the deaths of household members. It works in conjunction with another AI program, "Lavender," which sweeps through data from drone footage, intercepted phone calls, and geolocation devices. In Gaza alone, "Lavender" was said to have monitored more than 37,000 people. As of 16 April 2025, more than 51,000 Palestinians have been reported killed, according to Al Jazeera (Pietromarchi et al., 2025).

All the above examples of data misuse demonstrate both the potential and peril of data systems and prove that data neutrality can be masked by systemic bias. These are not flaws in the data itself but rather failures of transparency and, at times, a lack of capacity or willingness to question and challenge how data is used. Thus, it can be said that the answer to data neutrality is strong governance informed by efficacious policy. Europe's General Data Protection Regulation (GDPR) is considered to be the gold standard when it comes to how data can be used to enhance institutional accountability and, consequently, public acceptance of the extensive use of data in everyday life (European Data Protection Supervisor, n.d.). Many countries' national data policies have been modelled on that, including that of Türkiye. Another way to achieve effective governance is to ensure that organisations implementing auditing tools for both data and models are operating fairly across all population groups and that anyone can interpret and contest the resulting outcomes, particularly when it comes to hiring, lending, access to services, et cetera. There should be government bodies that overlook these institutional and organisational audits to provide fair compensation, as well as ensure model recalibration if any data-related harm is found to have been inflicted, and, ideally, regular audits for these government bodies as well.

With that said, Shoshana Zuboff's "Surveillance Capitalism" (Zuboff, 2019, p. 14) comes to mind recontextualising the neutrality of data as a fictional theory maintained by the opacity of proprietary algorithms and extraction-driven

business models that may benefit the state itself. She argues that user behaviour on social media is inherently autonomous and only becomes commodified through the retroactive appropriation and monetisation of personal data by platform companies. Related to this is "Platform Capitalism" (Srnicek, 2017), which captures how digital infrastructure has become a vehicle for data-driven profit extraction (Srnicek, 2017). Srnicek argues that platform capitalism is "a new way of accumulating capital" (Srnicek, 2017, p. 36) based upon a "massive new raw material to appropriate: data" (p. 88). Both Zuboff and Srnicek describe how behavioural data is monetised by turning users into sources of predictive products for state actors as well, similar to advertisers.

Given that, it is highly likely that states are not willing to police themselves or hold themselves accountable if they are the ones benefiting from misusing data to achieve particular objectives. Security is often considered a valid enough reason to misuse data to suppress human rights. Across jurisdictions, governments deploy the language of safety to justify mass surveillance, predictive policing, biometric tracking, and algorithmic border control (European Parliament, 2024). This securitisation of data governance creates a permissive environment where rights are subordinated to risk, especially the risks defined by the state.

As Foucault stated, modern power often functions not through overt coercion but through the normalisation of surveillance as care. When surveillance is framed as protection, especially in the name of national security, it becomes culturally palatable and, at times, even desirable. Nevertheless, beneath this veneer lies a disciplinary regime that renders entire populations visible, sortable as well as governable, often without their consent. Then, data neutrality becomes a rhetorical tool rather than a technical reality as decisions about whom to watch, what to flag and how to intervene are very political in nature.

To Whom Does Data Belong?

Data ownership, i.e. who owns the data, consequently, becomes critically important (Ruppert, Isin & Bigo, 2017). User activity transforms into proprietary information, which is exploited by technological behemoths such as Meta, Amazon, and Google for profit. Fundamental concerns, such as the following, are raised:

- If people create information through their actions, should they not own it?

  If people generate data through their actions, they should arguably have ownership over it. Yet, current systems favour platforms and governments that collect and monetise this data. Every action people perform on the internet, such as clicks, searches, and postings, creates data that drives the digital economy. Platform dominance, unclear or exploitative terms of service, and legal loopholes lead to users not having any say in their own data.

- If people create information through their actions, shouldn't they gain from its value?

  Tech giants such as Meta and Google profit from user-generated data by offering targeted advertisements and enhancing their services, raking in colossal revenues in the process. However, most users, the actual people creating this data, do not earn anything tangible. In terms of fairness and consent, this is clearly an ethical issue.

- Should information on public activity (for example, city movement) be stored in unidentified foreign-controlled cloud systems?

It is risky to store public activity information, like city movement patterns, in cloud systems operated by foreigners. This type of data may contain sensitive details regarding national assets or private citizen information. Once stored in foreign jurisdictions, the information is under the control of foreign laws and possible eavesdropping, which undermines national sovereignty and privacy. In addition, using foreign cloud services may result in weaknesses such as unauthorised access and data breaches.

The Global South is increasingly taking an interest in data sovereignty to keep data that is created on their territory in national hands. At the same time, the EU's GAIA-X project proposed a federated, European-owned cloud infrastructure to lower dependence on American technology platforms (van der Schaaf, Hertweck & Moßgraber, 2022). In the meantime, academics suggest data trusts, i.e. organisations that possess and control data on behalf of a specified group, subject to fiduciary obligations, can be created. These forms can redistribute control in favour of citizens, putting data used in alignment with community interests instead of corporate gain. Short of a change in ownership, neutrality is difficult to attain since unaccountable authorities can weaponise information in ways that are invisible and irreversible.

Towards a Digital Social Contract: When Data Rules, What Rules Data?

These evolving models of data governance, from national sovereignty to fiduciary trusts, reflect a growing realisation about data being a political asset alongside a technical one. As both individuals and communities demand greater agency over how their data is used, a foundation of shared ethical values surrounding data is needed. This brings about a deeper question: if data now mediates everything from pandemic control to college admissions, then what rules should govern its rule? In response, the case emerges for a new digital social contract. Such a contract would establish what rights people have over their data, what responsibilities institutions have in its utilisation, and, importantly, which public purposes justify exceptional use. Basic principles could be:

Data Dignity: Every human being should have the right to decide how information about them is used. It is based on the belief that personal data is a part of one's identity and that one needs to have control over its collection, usage as well as dissemination. Current practices where companies are looking to farm user data without consent or payment are considered to be ethical issues that need resolution.

Collective Governance: Collective high-stakes applications of data (for example, in welfare and policing) need to be co-governed by impacted communities and the public sector. This makes data-informed choices transparent, inclusive and responsive to community values and needs. It promotes participatory decision-making processes, making decisions less vulnerable to bias and systemic injustices.

Mutual Value: It is considered ethical practice to return value to communities from which information has been gathered, whether that is more access to governance or decision-making, actual monetary benefit, or any other benefit. This would ensure higher trust in a mutually beneficial relationship, as well as continued or expanded data sharing in the form of volunteering for data-sharing initiatives.

This stance neither fetishises nor fears information. It considers information infrastructure potent, necessary, and in need of constant democratic control. Just as physical infrastructures such as utilities and roads form the foundation for societal operation, digital information systems are the underlying frameworks of contemporary life. They inform healthcare, educational, governmental, and commercial decisions. Conceptualising information as infrastructure clarifies its role as a public good that must be controlled, tended and open to all. The implementation of the above key principles turns data from a commodity for exploitation into a resource governed for the common good. Needless to say, this paradigm shift necessitates continuous democratic stewardship, in which practices and policies are forged through accountability and public engagement. By framing and addressing data as infrastructure, its inherent value to society can be recognised and managed in a way that upholds democratic ideals and serves the interests of all.



(Abdullah Güçlü - Anadolu Agency)

Blockchain as a Potential Foundation for a Democratic Data Infrastructure

Given that data is becoming the infrastructure of operations across societies, from education to public health programs, blockchain technology potentially offers a viable mechanism to underpin such an infrastructure, augmenting the above-mentioned principles forming the basis of a digital social contract: data dignity, collective governance, and mutual value (Esposito & Araral, 2025).

Firstly, due to the decentralised nature of blockchain technology, individuals own their own data. Moreover, smart contracts can enable a predefinition of conditions that can allow access and utilisation of said data, where consent is not just expressed but is highly enforceable, which is very much in line with the concept of data dignity. Secondly, in terms of collective governance, the immutable nature of blockchain technology ensures that all data transactions are transparent and non-tamperable. This is critical when it comes to governance structures of all kinds, but especially in the context of data infrastructure. For example, all users need to know how data is being used by a public institution such as the police for increased accountability and acceptability, as audit trails create trust. Another use of blockchain technology for collective governance is Decentralised Autonomous Organisations (DAOs), which facilitate decentralised decision-making by requiring stakeholders to be directly involved in governance so that data systems are governed democratically (Tapscott & Tapscott, 2016; Allen & Berg, 2020).

Finally, when it comes to the creation of mutual value, blockchain technology is able to support data systems where data contributors can benefit directly from the value they create. An example of this is Farcaster, which is a decentralised social media protocol emphasising user privacy, autonomy and censorship resistance. It also allows its users to receive compensation for content as well as interactions, creating an ecosystem of mutual value generation (Coinbase, n.d.). All three features of blockchain technology (including being decentralised, immutable and focused on mutual value creation) can reorient data practices toward democratic values in a way that makes information serve the public good and not merely corporate interests.

Conclusion

Instead of asking whether data is good or bad, it is more important to ask who has the power to collect, access, and act on data. Equitable data governance means foregrounding human rights, ensuring transparency in algorithmic systems, and developing participatory mechanisms that reflect diverse publics. While data itself can be considered neutral, maintaining this neutrality requires concerted effort. Neutrality must be designed into systems, safeguarded by laws, and underpinned by transparency and accountability for all stakeholders. Without this, data systems risk deepening digital authoritarianism and technocratic exclusion.

In this context, blockchain technology potentially emerges as a promising tool to develop democratic data infrastructures, featuring decentralisation, immutability, and the ability to create mutual value. All stakeholders' goal should be to make data work for society, not the other way around. By embedding principles of fairness, transparency, and collective benefit into our digital frameworks and then leveraging technologies like blockchain to support these principles, a more equitable and just digital society and world can be built.

References

Abraham, Y. (2024, April 3). *'Lavender': The AI machine directing Israel's bombing spree in Gaza*. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

AFAD. (n.d.). Earthquake and disaster data systems. Disaster and Emergency Management Authority of Türkiye. https://www.afad.gov.tr

Allen, D., & Berg, C. (2020). Blockchain governance: What we can learn from the economics of institutions. *Journal of the British Blockchain Association*, 3(2), 1–10.

Benbouzid, B. (2019). To predict and to manage: Predictive policing in the United States. *Big Data & Society, 6*(1), 1–6. https://doi.org/10.1177/2053951719861703

Botsman, R. (2017, October 21). *Big data meets Big Brother as China moves to rate its citizens*. WIRED. https://www.wired.com/story/chinese-government-social-credit-score-privacy-invasion/

Coinbase. (n.d.). *What is the decentralized social media platform Farcaster?* Retrieved April 16, 2025, from https://www.coinbase.com/learn/crypto-basics/what-is-the-decentralized-social-media-platform-farcaster

Esposito, M., & Araral, E. (2025, February 7). The digital commons: How to harness blockchain for better governance. *World Economic Forum*. https://www.weforum.org/stories/2025/02/digital-commons-blockchain-governance/

European Data Protection Supervisor. (n.d.). *History of the General Data Protection Regulation*. Retrieved April 16, 2025, from https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

European Parliament. (2024). *Artificial Intelligence and Human Rights: The Impact of AI on Fundamental Rights in the EU* (Study No. 754450). Directorate-General for External Policies. https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf

Foucault, M. (1980). *Power/knowledge: Selected interviews and other writings, 1972–1977* (C. Gordon, Ed.). Pantheon Books.

Fraser, N. (2003). Social justice in the age of identity politics: Redistribution, recognition, and participation. In N. Fraser & A. Honneth, *Redistribution or recognition? A political-philosophical exchange* (pp. 7–109). Verso.

Gitelman, L., & Jackson, V. (2013). Introduction. In L. Gitelman (Ed.), *"Raw data" is an oxymoron* (pp. 1–14). The MIT Press.

Johnson, T. L., & Johnson, N. N. (2023, May 18). *Police facial recognition technology can't tell Black people apart*. Scientific American. https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/

Milan, S., & Treré, E. (2024). *The asymmetry of access to public data*. Retrieved from: https://www.researchgate.net/publication/388333749_The_Asymmetry_of_Access_to_Public_Data

Pietromarchi, V., Jamal, U., Siddiqui, U., & Kestler-D'Amours, J. (2025, April 16). *LIVE: Hamas says no ceasefire if no Israeli withdrawal from Gaza*. Al Jazeera. https://www.aljazeera.com/news/liveblog/2025/4/16/live-israeli-forces-systematically-destroying-homes-in-gaza:contentReference[oaicite:0]{index=0}

Republic of Türkiye Digital Transformation Office. (n.d.). e-Devlet Kapısı (E-Government Gateway). https://www.turkiye.gov.tr

Rosenberg, M., Confessore, N., & Cadwalladr, C. (2018, March 17). How Trump consultants exploited the Facebook data of millions. *New York Times*. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big Data & Society, 4*(2), 1–7. https://doi.org/10.1177/2053951717717749

Srnicek, N. (2017)**.** *Platform capitalism*. Polity Press.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world*. Penguin.

van der Schaaf, H., Hertweck, P., & Moßgraber, J. (2022). *INSPIRE - Gaia-X Use Cases: Final Report* (Version 1.1). Retrieved from https://docs.gaia-x.eu/

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.