The Risks of Data Use : an ethical perspective

Introduction

Risk, in the context of data, refers to the possibility of a negative outcome arising from the collection, processing, and use of information. These risks, which may include privacy violations, algorithmic discrimination, and threats to autonomy, demand ethical scrutiny, particularly in public administration where data-driven systems directly impact citizens. From an ethical perspective, risk can be approached through different lenses. A consequentialist perspective evaluates risk by focusing on the outcomes of actions, emphasizing the importance of minimizing harm and ensuring equitable benefits. This approach prompts an analysis of how data systems influence individuals and communities, both positively and negatively.

In contrast, Kantian ethics centers on the inherent dignity of individuals, advocating for respect for every person as a unique being with their own identity and autonomy. In the context of data, this perspective underscores the ethical obligation to treat individuals as ends in themselves rather than as mere means to an organizational goal. These dual perspectives—thinking about consequences and respecting human dignity—are essential for understanding the ethical dimensions of risk in data systems.

Luciano Floridi's concept of the infosphere adds another layer of complexity to this analysis. The infosphere represents the interconnected environment of digital and physical realities where individuals, as informational organisms (inforgs), interact with data systems that shape their autonomy and societal roles (Floridi, 2014). This integration of digital and physical spheres amplifies the ethical stakes, as risks in data systems affect not only individual users but also broader societal structures. By combining consequentialist and Kantian perspectives with Floridi's insights, this section aims to provide a comprehensive ethical analysis of risks in data systems, complementing technical and organizational considerations with a focus on fairness, transparency, and respect for autonomy.

Privacy and Informational Autonomy

Privacy is a foundational principle in the ethical governance of data systems. It is not merely a matter of confidentiality or secrecy but encompasses broader concerns related to informational autonomy. Informational autonomy refers to the ability of individuals to maintain control over their personal data and how it is used to shape their identity and interactions within society. Floridi emphasizes that privacy is a precondition for personal and societal well-being in the infosphere, as it allows individuals to define and protect their informational boundaries (Floridi, 2014).

The philosophical foundations of privacy have evolved over centuries, with roots in Aristotle's distinction between the public and private spheres. In modern contexts, privacy is understood as both a spatial and informational concept. Spatially, it refers to the boundaries of private life, such as personal spaces and domestic environments. Informationally, it pertains to the control over how personal data is collected, shared, and utilized (Gharib & Mylopoulos, 2021). Ethical risks arise when municipalities deploy technologies such as facial recognition systems or integrate sensitive data into centralized systems. These practices often blur the boundaries between public and private life, undermining citizens' ability to manage their informational autonomy.

To address these risks, municipalities must adopt ethical frameworks that prioritize transparency, informed consent, and accountability. Floridi's concept of soft ethics offers a pathway for achieving this by emphasizing the proactive embedding of ethical values into the design and governance of data systems. Soft ethics moves beyond mere legal compliance to ensure that privacy is respected as an essential human right and societal value (Floridi, 2018).

Algorithmic Bias and Discrimination

Algorithmic systems play a central role in public administration, from resource allocation to decision-making in welfare programs. While these systems can improve efficiency, they often inherit and amplify biases embedded in their training data. Algorithmic bias occurs when historical inequities, societal stereotypes, or incomplete datasets shape algorithmic outputs, leading to discriminatory outcomes. These risks are particularly acute in systems that make high-stakes decisions about individuals, such as determining eligibility for social benefits or identifying individuals for law enforcement scrutiny.

The Dutch childcare benefits scandal is a stark example of the consequences of algorithmic bias. In this case, biased algorithms flagged families for fraud based on discriminatory criteria, such as dual nationality and foreign-sounding names. The impact was devastating: thousands of families faced unjust accusations, financial hardship, and emotional distress (Zuboff, 2019). This scandal not only exposed the technical flaws in the algorithm but also highlighted the ethical failures in its design and governance.

Addressing algorithmic bias requires a multifaceted approach. First, data systems must be designed with fairness as a core principle. This includes curating diverse and representative datasets to minimize the risk of bias. Second, regular audits of algorithms and their outputs are essential to identify and rectify discriminatory patterns (Floridi, 2018). Third, inclusive governance processes that involve diverse stakeholders can ensure that the values and needs of all communities are considered during the development and deployment of data systems.

Floridi highlights that fairness and accountability are not optional in the governance of algorithmic systems. They are ethical imperatives that ensure these systems serve the public good. Ethical frameworks must be embedded into the lifecycle of data systems to prevent harm, promote equity, and maintain public trust in government institutions (Floridi, 2014).

Autonomy and Manipulation

Autonomy is another critical ethical dimension in the analysis of data risks. Autonomy refers to the capacity of individuals to make informed and independent decisions. However, data systems that rely on predictive analytics and behavioral targeting often undermine this capacity by influencing behavior in subtle but significant ways. These systems are designed to nudge individuals toward specific actions, often without their awareness or consent.

Harari highlights the manipulative potential of data-driven systems, particularly in contexts where they exploit personal information to shape choices (Harari, 2018). For example, targeted advertising and behavioral interventions in public services may limit individuals’ ability to act freely by steering them toward predetermined outcomes. This raises ethical concerns about the transparency of such systems and the degree to which they respect the autonomy of their users.

In the infosphere, autonomy is closely linked to the design and governance of data systems. Floridi argues that systems must be designed to empower individuals rather than constrain their agency.

This involves providing citizens with meaningful choices, ensuring that systems operate transparently, and enabling individuals to understand and contest algorithmic decisions. Autonomy-preserving design is essential for ensuring that data systems do not merely optimize for efficiency but also respect the values and preferences of the communities they serve (Floridi, 2014).

Governance and Regulatory Standards

Governance and regulatory frameworks are crucial for addressing the ethical risks associated with data systems. While laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) provide baseline protections for privacy and data security, they must be adapted to the unique contexts of municipalities and local governments. These regulations empower individuals with rights over their personal data, including the ability to access, delete, and control its use (European Commission, 2019). However, their effectiveness depends on the extent to which local governments implement and enforce these protections.

Floridi's concept of digital environmentalism underscores the importance of sustainable data practices that preserve the integrity of the infosphere. This involves adopting governance models that integrate ethical principles such as fairness, transparency, and accountability into the design and management of data systems. By aligning with global standards while addressing local needs, municipalities can ensure their data practices reflect the values of the communities they serve (Floridi, 2014).

Bibliography

European Commission. (2019). *Ethics Guidelines for Trustworthy AI*. Retrieved from https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

Floridi, L. (2011). *The Philosophy of Information*. Oxford University Press.

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford University Press.

Floridi, L. (2018). *Soft Ethics and the Governance of the Digital*, in *Philosophy of Technology* 31: 1-8.

Gharib, M., & Mylopoulos, J. (2021). *On the Philosophical Foundations of Privacy: Five Theses*. Springer.

Harari, Y. N. (2018). *21 Lessons for the 21st Century*. Spiegel & Grau.

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