CYBER STRATEGY & POLICY: POLICY ANALYSIS PAPER 3

Ean N. Miller

Old Dominion University

CYSE 425W: Cyber Strategy & Policy

Professor Teresa Duvall

October 11, 2024

The influence of the EU's General Data Protection Regulation has incredibly hit how personal information is handled worldwide, giving way to a complete framework that secures the rights of individuals about privacy and data protection. In general, these come with several ethical issues, such as the balance of the rights of individuals against business interests, compliance costs, and more significant implications for society from strict data protection standards.

One of the most significant ethical benefits of the GDPR is the reinforcement of individual autonomy and the right to privacy. It enshrines a right to access, rectification, and erasure of data subjects over their data, ensuring that they have more control over the information concerning them. It puts power back into the hands of an individual in a world where personal data has become some form of currency, saving them from misusing their information by organizations. This is with ethical principles of informed consent and transparency, where organizations under the GDPR are compelled to inform individuals clearly of the collection and processing of their data.

Also, with the regulation, there is the "privacy by design" aspect, which implies that at the design phase, privacy will be built into systems and processes to avoid potential breaches even before they occur. This helps increase confidence among consumers and organizations, as a given organization is expected to ensure that data protection is an integral part of its processes, thus further minimizing data exploitation even more. (Florea & Florea, 2020).

While it's true that the GDPR does carry some specific advantages, it also places significant ethical difficulties on businesses. It requires a lot of money to comply with the regulations. The smaller ones, especially SMEs, can only sometimes afford the immense requirements of the GDPR, and they have to hire data protection officers, conduct privacy impact assessments, and upgrade their management systems. This raises questions of fairness since the smaller firms could hardly be in a position to comply, therefore creating a barrier to effective competition or innovation in the marketplace.

Furthermore, the focus of the GDPR on personal data protection, concerning making data available for research, is very minute, considering the vast datasets in healthcare that allow scientific improvements. Concerning ethical dilemmas, balancing personal privacy with public interest may prevent medical researchers from looking into the basis of diseases and developing life-saving treatments. This tension underlines the moral complexity of the GDPR, as it needs to balance competing values of privacy and societal benefit.

The GDPR is based on the principle that one of the basic rights of human beings is a right to privacy, for which protection is to be guaranteed under the law. It allows the individual to be in control of their personal information and can identify who has access to their information and for what purpose. Simultaneously, the same regulation limits such rights when organizations are compelled to process data for legitimate business interest purposes or public safety reasons.

For example, the "right to be forgotten" is the epicenter of the GDPR, but it is never absolute. It can also be refused when an organization has a legal requirement to retain the data or for a legal claim, establishing how such rights could infringe upon an individual's right to privacy. This raises ethical issues regarding the weighing of individual rights against the needs of

businesses and public authorities in many instances in which privacy conflicts with other societal interests, such as public health or security. (Hijmans & Raab, 2018).

The GDPR is a very positive ethical step forward for protecting privacy rights in the Digital Era. It gives people more control over their personal information, thus engendering transparency and accountability in organizations. Nevertheless, the regulation is criticized for being overly burdensome, especially for smaller businesses and researchers. The tradeoff between privacy rights and benefits that society derives from access to information remains one of the thorny ethical issues; hence, the need for a critical framework like the GDPR.

References

Fanaei Sheikholeslami, D., Alves, P., & Hassanzadeh Benam, A. (2023). *Artificial Intelligence Ethics and Challenges in Healthcare Applications: A Comprehensive Review in the Context of the European GDPR Mandate*. MDPI. https://doi.org/10.3390/make5030053

Florea, D., & Florea, S. (2020). *Big Data and the Ethical Implications of Data Privacy in Higher Education Research*. MDPI. https://doi.org/10.3390/su12208744

Hijmans, H., & Raab, C. D. (2018). *Ethical Dimensions of the GDPR*. European Data Protection Law Review, 4(2), 155-170. https://doi.org/10.21552/edpl/2018/2/6