Dignity by Design: Meeting the Challenge of Data Technologies to the Deep Values of the Legal Order

By Viraansh Bhanushali

Introduction

Data technologies are said to challenge the ‘deep values’ of liberty, equality, and justice on which our legal order rests. Through practices like surveillance capitalism and algorithmic decision-making, these technologies erode individual autonomy and compromise human dignity.

On the legal order

In the Kelsenian conception, a legal order is not merely a collection of norms (oughts) but a hierarchical system where each norm derives its validity from a higher norm, ultimately culminating in a basic norm or Grundnorm.[1] If the law is seen as a positive endeavour, the norms of legal order are "posited" or "created" through legislative acts, legally binding orders, judicial decisions, etc. These are considered legal acts, and the individuals and institutions authorised by the legal acts to carry them out are recognised as legal officials and institutions that constitute our contemporary legal and regulatory authorities.[2]

On Values

The legal order is unique in its ability not only to establish norms in society but also to enforce them with a socio-moral monopoly on the use of force. As Brownsword argues, the ascription of the legal order to “deep values” grants it this monopoly, which in turn gives it legitimacy.[3]

Düwell argues that respect for human dignity forms the basis for the legitimacy of the legal order and emphasises that human dignity is not a value, but a status rooted in the universal human capacity for agency—the ability to set goals and act autonomously.[4] This capacity, shared by all human beings, creates a reciprocal obligation to respect the dignity of others. This respect necessitates the recognition of equality. Jeremy Waldron argues that the idea of human dignity is intimately connected to the principle of equal moral worth.[5] He explains that dignity historically

[1] Kelsen-1982, Page 64

[2] Ibid.

[3] Brownsword-2017, page 7

[4] Düwell-2017, page 181

[5] Waldron-2012, page 47

referred to rank or status, but in modern legal contexts, it signifies that all individuals possess an inherent worth demanding equal respect and consideration.[6]Dworkin connects human dignity to justice and liberty, with justice requiring the state to treat all those in its charge with equal concern and respect,[7] and Rawls describes a just legal order as one that not only upholds individual liberties but also ensures that these liberties are equally distributed.[8]

Thus, the deep values upon which our legal order rests—equality, justice, and liberty—are interwoven and rooted in the protection of human dignity. These values are not isolated pillars but are interconnected principles that collectively underpin the legitimacy of the legal system.

The rise of data technologies challenges these pillars. Data technologies are systems that collect, process, and analyse large volumes of data to make decisions or insights which are relied upon in decision-making processes. The expansive data gathering at the heart of these technologies challenges our liberal, just, and equal legal order.

The Challenge

Zuboff argues these technologies have enabled a new economic order where personal data extracted through surveillance becomes a primary commodity, Surveillance Capitalism.[9] Unlike traditional capitalism, which revolves around the exchange of goods and services, surveillance capitalism thrives on the continuous collection, analysis, and commodification of personal information. Like the rise of traditional capitalism, the rise of surveillance capitalism has transformed both the nature of commerce and the commercial entities that operate it in its paradigm.

Sterling describes this as a cybernetic consortium for control of property, where corporations of today no longer compete for consumption of their products but instead the data of their consumers.[10] This has led to the rise of data brokers, who act as intermediaries in the commodification process by collecting, analysing, and selling vast amounts of personal data

[6] Ibid.

[7] Dworkin-1977, page 199

[8] Rawls-1972, page 266

[9] Zuboff, 2015, page 75

[10] Sterling-2014

without individuals' explicit consent.[11] This commodification of personal data dehumanises individuals, reducing them to data points rather than recognising their agency and moral worth.

This commodification has led to what Cohen calls the biopolitical domain, where the entire consciousness of individuals is seen as property, available for commerce.[12] Data brokers have now turned into data refineries, which are now capable of producing data doubles—virtual representations of individuals that are meticulously optimised to predict and influence their choices and behaviour.[13] These data doubles enable companies and governments alike to engage in 'behavioural modification'. For example, by analysing a user's browsing history and social interactions, platforms can predict emotional states and deliver content or advertisements that capitalise on those emotions, steering decisions without the user's conscious awareness. This has led to scenarios where convenience stores have been able to know that an individual was pregnant even before they did and attempt to influence their consumption choices. [14]

As data technologies continue to infiltrate the fabric of society, instead of changing the laws that govern behaviour, they can now simply "code out" our choices. Brownsword refers to this as Technological management, arguing that as a result, individuals, while still having normative liberty, lose their practical liberty. [15]

Take, for example, Amazon's use of its algorithms and data technologies to shape consumer behaviour. Amazon's recommendation system uses personal data, including purchase history, browsing patterns, and even behavioural predictions from a user's "data double".[16] The platform does not just predict what users might want; it subtly pushes them toward products that maximise its profits, often its own 'Amazon Basics'.[17] While users conceptually have the normative liberty to purchase from other brands or platforms, their practical liberty to exercise that choice is undermined by a system that makes alternatives less visible, less convenient, or less appealing. The algorithm has already made the "real" choice for them, not by explicit coercion, but by narrowing the practical range of options effectively available. Brownsword refers to this as

[11] Reviglio,2022, page 2

[12] Cohen, 2018, page 214

[13] Ibid, page 224

[14] Hill, 2012

[15] Brownsword-2017, page 42

[16] Harding, 2015

[17] Ibid

“paper liberty”—a nominal freedom of choice that lacks any substantive capacity for action.[18] When data technologies control and influence individual behaviour without transparency or consent, they undermine our agency.[19]

The ability of data technologies to erode practical liberty at will effectively grants them carte blanche to shape and influence our normative frameworks. By subtly managing behaviours, limiting “real” choices and manipulating both the environment in which choices are made and the choices themselves, they challenge the very integrity of our value of liberty.

The impact of data technologies extends beyond individuals to the very systems designed to uphold justice, which are also vulnerable to distortion through the permeation of the avenues of justice delivery. From the courts that interpret and apply legal norms to the tools utilised by legal practitioners, data technologies are pervasive. Legal Information Systems (LIS) such as Westlaw and LexisNexis have made legal resources more accessible than ever before, with lawyers, judges and legislators alike relying on them as authoritative sources of legal information. While these advancements have been widely praised for addressing pragmatic challenges faced by the judiciary—such as providing easy access to legal information and reducing time-based barriers to justice—their integration raises serious concerns about perverting the very notion of justice and the processes with which it is delivered.

In 2024, in line with industry trends, Lexis introduced Lexis+AI, an artificial intelligence legal research tool that allows individuals to leverage AI models for searching case law and drafting submissions.[20] This is only indicative of a larger drive to integrate AI by LISes, with analogues by LISes like Casemine and Westlaw. With the rise of such tools, data technologies have moved from being mere procedural tools to sources of information and means of information gathering.

Artificial intelligence models like those used in Lexis+AI function as "black boxes."[21] Unlike traditional, linear algorithms, these machine learning models process information in ways fundamentally different from human cognition, leading to a form of "technological illiteracy"

[18] Brownsword-2017, Page 45

[19] Düwell-2017, page 183

[20] Magesh et al. 2024

[21] Carabantes, 2019, 310-312

among users.[22] Even though the AI's output may seem coherent and reliable, the reasoning it uses to reach its conclusions remains opaque—even to its creators.[23]

This opacity becomes particularly concerning when coupled with AI's propensity to inherit and propagate biases from the data on which it is trained.[24] These models have shown that these models can exhibit biases toward certain values, ideas, and political ideologies, which are pervasive in their outputs.[25] This leads to a scenario where, when the search engine and the jurisprudential database are functionally simplified and closed in a search algorithm, it can become extremely difficult for the user to ascertain whether the search system is truly neutral or the jurisprudence database is complete.[26] Together with the fact that industry-standard LISes provide these models, it becomes nearly impossible for users to even identify the biases present in the outputs of these models because of a tendency to consider the AI systems output as legitimate because it is provided by a LIS that is considered legitimate. Empirical evidence shows that users who interact with biased AI systems may unconsciously adopt those biases, influencing their future decisions even after they stop using the AI.[27] This effectively allows the creators of these algorithms to usurp the role of 'delegates' and act without the veil of ignorance in Rawls's theory of justice.[28] When algorithm creators design AI models like Lexis+AI, they select and prioritise datasets with full knowledge of their societal positions and interests, acting without a veil of ignorance. They have the power to choose which principles and values to prioritise in their datasets while knowing their place in society. This gives them undue influence over the principles underpinning our conception of justice.

Data technologies' insights that inform decisions are not limited to merely informational systems in the legal practice but also in governance by institutions of the legal order. Law enforcement agencies in the United States have adopted data mining algorithms to predict potential criminal activity, a practice known as predictive policing. A notable example is the Los Angeles Police Department's (LAPD) implementation of PredPol, a system that uses historical crime data to

[22] Ibid.

[23] Ibid.

[24] Rozado-2023

[25] Ibid.

[26] Mangesh et al-2024

[27] Vicente et al-2023,

[28] Rawls-1972, page

forecast where crimes are likely to occur.[29] PredPol analyses vast amounts of data, including arrest records, incident reports, and time and location of past crimes, to identify potential crime hotspots.[30]

The algorithm operates by applying machine learning techniques to historical crime, socio-economic, and health data received from data mining municipal records to predict future crime locations. Officers are then deployed to these predicted hotspots to deter criminal activity. The system is preferred for its ability to allocate police resources more efficiently and potentially reduce crime rates by preventing crimes before they occur. [31]

When an individual is flagged as residing in a predicted crime hotspot, they may experience increased stops, searches, and surveillance solely based on their location rather than any personal culpability.[32] This heightened policing fosters anxiety and tension within already marginalised communities, potentially exacerbating the very issues of crime and unrest that such technologies aim to mitigate.[33] The individuals affected are subjected to unequal treatment, not because of their actions but due to algorithmic determinations arising from data they often did not consent to be used in this way. This creates a system of unequal liberty, where the system of liberty an individual experiences is determined with the means of regulation via data technologies. Individuals do not retain an equal ability to shape the norms that govern them, this governance by data technologies puts this normative "data power" in the hands of a select few.[34] Moreover, when individuals are subjected to differential treatment based on algorithmic biases, their inherent dignity is compromised.

The common denominator in these criticisms is that data technologies fundamentally violate human dignity. For instance, the commodification of personal data, as seen in surveillance capitalism, reduces individuals to data points, stripping them of their autonomy and transforming them into objects for commercial exploitation. This diminishes their capacity for agency, as their decisions are influenced by algorithmic systems that serve corporate interests rather than their

[29] Santos-2019

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] Gormally et al-2012

[34] Lynskey-2019

own. Similarly, predictive policing data technologies like PredPol, which target individuals based on their location rather than personal culpability, undermine their dignity by subjecting them to unequal treatment and surveillance without the ability to contest it within our legal order. These practices compromise individual agency by restricting the ability to make free, fair, and informed decisions.

Meeting the Challenge

Meeting the challenge posed by data technologies requires inverting Lessig's famous proclamation that "code is law."[35] While Lessig recognised that technology has the power to regulate human behaviour outside of legal frameworks, this power has increasingly compromised fundamental human values like dignity and agency. To address these issues, the law itself must become code, embedding legal principles into the very architecture of the digital technologies that shape our lives.

Hildebrandt's doctrine of Legal Protection by Design (LPbD) provides the means to achieve this, ensuring that data technologies respect human dignity, protect individual agency, and uphold the values of liberty, equality, and justice.[36] LPbD integrates legal protections. Unlike passive legal approaches that impose rules after technologies are established, LPbD's expansion can ensure that the protection of human dignity is a proactive, built-in feature of data technologies and their development, creating a doctrine of Dignity by Design (DbD).

For example, systems must be designed to offer users clear, meaningful choices about how their data is collected and used. Rather than simply steering users through opaque algorithms, platforms like Amazon and Google would be required to give users control over whether their experience is shaped by personalised algorithms or by neutral, non-intrusive systems. This restores a measure of dignity by allowing individuals to make informed, autonomous decisions about how they interact with data technologies.

LPbD is already in practice in some jurisdictions, most notably in the European Union. Article 25 of the GDPR requires that privacy be embedded into systems from the outset, ensuring that data

[35] Lessig-1999

[36] Hildebrandt-2020,

is minimised and used only for its intended purposes.[37] Data Protection Impact Assessments (DPIAs), mandated by Article 35, require organisations to take proactive measures to assess the risks posed by their data technologies and to implement safeguards to protect the rights of individuals.[38] These principles not only prevent the abuse of personal data but also ensure that individuals retain control over their information.

However, even with transparency, the power imbalance between users and platforms that Zuboff mentions remains intact.[39] For instance, platforms like Amazon may give users the option to opt out of personalised algorithms, but users may still struggle to understand the full extent of data collection and its influence on their decisions. In this case, transparency alone may not be enough to restore autonomy.

Drawing from existing norms of the legal order, DbD can be amended to include requirements that require data technology institutions to meet objective standards: would two reasonable individuals, when presented with all relevant information, come to the same understanding of how the system collects and processes their data? This approach ensures that transparency is not just a matter of disclosing information but of making it comprehensible and meaningful to users. By applying this standard, our amended methods of DbD ensure that individuals are truly informed in the choices they make over their data, enhancing their autonomy and protecting their dignity.

However, what about informing users about the algorithms used in our earlier examples of Search engines and Generative Artificial intelligence? These are said to be black boxes, not even the creators know how they come to the conclusions they do, so how can one expect the average "technologically" illiterate user to?

A proposed solution to this issue in the LPbD paradigm is the right to explanation, which is partially present in the GDPR. Articles 15 and 22 grant individuals the right to know how decisions are made by automated systems and, in some cases, to contest those decisions.[40] The

[37] Regulation 2016/679

[38] Ibid.

[39] Zuboff-2015

[40] Regulation 2016/679, s15 and s22

idea behind this right is to offer transparency and give individuals insights into how algorithmic decisions are made, thereby mitigating the risks posed by opaque technologies.

Despite its promise, the right to explanation in its current form is limited. One major issue is that it only applies to fully automated decisions, excluding scenarios where algorithms assist human decision-makers, like the ones in PredPol. This exclusion creates a loophole where individuals still face significant algorithmic influence without recourse to an explanation.[41] Moreover, the depth or clarity of explanations that should be provided is not specified, making it unclear whether a general description of the system is sufficient or whether detailed, case-specific insights are required.[42] This, once again, raises concerns about empowering technologists with the ability to decide the extent to which individuals have a right to explanation.

The LPbD provisions in the GDPR also fall short of addressing group-based algorithmic harms, like the ones in our case of PredPol. For instance, a loan approval algorithm disadvantaging certain racial groups due to data mined correlations that serve as proxies for race, even without explicitly considering race as a factor. Under the current provisions of the GDPR, there would exist no right of explanation in this scenario.[43]

DbD could address these LPbD issues via the development of more robust forms of explanation. Two key options are pedagogical explanations, which simplify complex algorithms into understandable terms, and counterfactual explanations, which illustrate what would have led to a different decision. For example, if an individual is denied a loan by an algorithm, a counterfactual explanation would inform them, “Had your income been higher by X amount, your application would have been approved.” This offers clarity without needing to expose the intricacies of machine learning models and allows individuals to challenge decisions effectively.

Another change could be expanding the right to explanation. Currently, under the GDPR, this right only applies to fully automated decisions. DbD would aim for expansion to include semi-automated processes, where algorithms influence human decision-makers. In instances like

[41] Edwards et al.-2017, page

[42] Goodman et al-2017, page

[43] Ausloos et al, 2022

hiring, where algorithms assist in ranking candidates, individuals should have the right to understand how the algorithm influenced the decision.

DbD would also advocate for systemic approaches to tackling algorithmic bias and implementing algorithmic audits, where independent organisations assess whether algorithms produce biased outcomes across demographic groups. These audits help identify systemic discrimination that may not be visible at the individual level. DbD also advocates for the mandatory use of bias detection tools during the development and deployment of algorithms, ensuring continuous monitoring of discriminatory effects.[44] Additionally, the introduction of collective redress mechanisms, like the Class action lawsuit used in some common law systems, would allow groups affected by similar algorithmic biases to seek remedies together. [45]

Thus, Dignity by Design offers a robust framework for meeting the challenges posed by data technologies by prioritising the protection of human dignity and individual agency. By embedding legal norms directly into the architecture of digital systems, DbD ensures that data technologies strengthen the deep values on which our legal order rests by respecting the dignified status of all human beings. Through principles of transparency, contestability, and democratic participation, DbD acts as our means to the end of establishing the respect of human dignity by data technologies via strengthening the deep values of liberty, equality, and justice on which the legal order rests.

Conclusion

The rise of data technologies presents a challenge to the deep values of the legal orders rests on—liberty, equality, justice, and, fundamentally, human dignity. These technologies, through practices such as surveillance capitalism, predictive policing, and algorithmic decision-making, threaten to undermine the agency and autonomy of individuals, corroding their ability to participate liberally and equally in a just society.

However, these challenges are not insurmountable. The doctrine of dignity by design offers a proactive framework to ensure that human dignity is respected and protected within the very fabric of data technologies. By embedding legal principles into the design and functioning of

[44] Nazer et al, 2023
[45] Ausloos et al, 2022

these systems, we can reclaim agency, foster transparency, and ensure that data technologies operate in service of, rather than in opposition to, the values that underpin our legal order.

Therefore, while the challenges posed by data technologies are significant, they can be met by integrating dignity by design into our legal and technological frameworks, thereby preserving the legitimacy of our legal order.

Bibliography

Ausloos, J., J. Toh and A. Giannopoulou (2022). "How the GDPR can exacerbate power asymmetries and collective data harms: To what extent are the GDPR's data rights an effective tool for enabling collective action?".

Brownsword, R., E. Scotford and K. Yeung (2017). 3Law, Regulation, and Technology: The Field, Frame, and Focal Questions. The Oxford Handbook of Law, Regulation and Technology. R. Brownsword, E. Scotford and K. Yeung, Oxford University Press**:** 0.

Carabantes, M. (2020). "Black-box artificial intelligence: an epistemological and critical analysis." AI & society **35**(2): 309-317.

Cohen, J. E. (2018). "The Biopolitical Public Domain: the Legal Construction of the Surveillance Economy." Philosophy & technology **31**(2): 213-233.

Düwell, M. (2017). 177 Human Dignity and the Ethics and Regulation of Technology. The Oxford Handbook of Law, Regulation and Technology. R. Brownsword, E. Scotford and K. Yeung, Oxford University Press**:** 0.

Dworkin, R. (1977). Taking rights seriously, Duckworth.

Edwards, L. and M. Veale (2017). "Slave to the algorithm? Why a'right to an explanation'is probably not the remedy you are looking for." Duke L. & Tech. Rev. **16**: 18.

Finnis, J. and J. Finnis (2011). 47Duties to Oneself in Kant. Human Rights and Common Good: Collected Essays Volume III, Oxford University Press**:** 0.

Goodman, B. and S. Flaxman (2017). "European Union regulations on algorithmic decision-making and a “right to explanation”." AI magazine **38**(3): 50-57.

Gormally, S. and R. Deuchar (2012). "Somewhere between distrust and dependence: young people, the police and anti-social behaviour management within marginalised communities." International journal on school disaffection **9**(1).

Hill, K. (2012). "How target figured out a teen girl was pregnant before her father did." Forbes, Inc **7**: 4-1.

Jones, T. and M. Maguire (1999). "Crime, community safety and the policing of marginalized populations: A review of research." Cardiff University.

Kelsen, H. and S. L. Paulson (1982). "The Concept of the Legal Order *." The American Journal of Jurisprudence **27**(1): 64-84.

Lessig, L. (1999). Code : and other laws of cyberspace. New York, Basic Books.

Lynskey, O. (2019). "Grappling with “Data Power”: Normative Nudges from Data Protection and Privacy." Theoretical inquiries in law **20**(1): 189-220.

Magesh, V., F. Surani, M. Dahl, M. Suzgun, C. D. Manning and D. E. Ho (2024). "Hallucination-Free? Assessing the Reliability of Leading AI Legal Research Tools." arXiv preprint arXiv:2405.20362.

Mika, K. (2022). "Friend or Foe? Lexis Artificial Intelligence (AI) in Legal Writing." Proceedings: Online Journal of Legal Writing Presentations **3**(1): 24.

Nazer, L. H., R. Zatarah, S. Waldrip, J. X. C. Ke, M. Moukheiber, A. K. Khanna, R. S. Hicklen, L. Moukheiber, D. Moukheiber and H. Ma (2023). "Bias in artificial intelligence algorithms and recommendations for mitigation." PLOS Digital Health **2**(6): e0000278.

Nazer, L. H., R. Zatarah, S. Waldrip, J. X. C. Ke, M. Moukheiber, A. K. Khanna, R. S. Hicklen, L. Moukheiber, D. Moukheiber and H. Ma (2023). "Bias in artificial intelligence algorithms and recommendations for mitigation." PLOS Digital Health **2**(6): e0000278.

Nichols, J. (2004). "Data doubles: Surveillance of subjects without substance." CTheory: 2-17.

Rawls, J. (1999). A Theory of Justice, Oxford University Press.

Reviglio, U. (2022). "The untamed and discreet role of data brokers in surveillance capitalism: A transnational and interdisciplinary overview." Internet policy review **11**(3): 1-27.

Rozado, D. (2023). "The political biases of chatgpt." Social Sciences **12**(3): 148.

Santos, R. B. (2019). "Predictive policing: Where's the evidence." Police innovation: contrasting perspectives: 366.

Vicente, L. and H. Matute (2023). "Humans inherit artificial intelligence biases." Scientific Reports **13**(1): 15737.

Waldron, J. and J. Waldron (2012). 47Law, Dignity, and Self-Control. Dignity, Rank, and Rights. M. Dan-Cohen, Oxford University Press**:** 0.

Zuboff, S. (2015). "Big other: Surveillance Capitalism and the Prospects of an Information Civilization." Journal of information technology **30**(1): 75-89.