Wilfried
Martens Centre
for European Studies

Reforming the EU's GDPR and AI Act:

Handling Data Power While Improving Competitiveness

Jan Czarnocki

Summary

December 2025

This policy brief argues that the General Data Protection Regulation (GDPR) should be refocused on the duty of loyalty in data relationships. This would allow a much-needed simplification of the Artificial Intelligence Act (AI Act). The purpose is to establish a regulatory focus on addressing the data power wielded by powerful entities online, while improving competitiveness. This can be achieved by the light-touch regulation of data processing entities that do not pose a significant risk to democracy and rights. The duty of loyalty requires that anybody processing personal data must act in the best interests of the people who may be affected by that processing. The higher the risk related to data processing, the greater the regulatory demands posed by the duty of loyalty. Such an approach would allow regulatory attention to focus on data power in the infosphere. Entities that hold such power should face strict duties and clear prohibitions; those that do not should meet only proportionate requirements.

Keywords GDPR – AI Act – Data power – GDPR reform – EU digital law – Constitutional governance

Introduction

The regulatory burden is one of the many reasons why the EU is less competitive and has fewer digital tech unicorns (startups valued above one billion euros) than the US and China. Besides creating a hostile atmosphere for starting a new business, regulations such as the General Data Protection Regulation (GDPR)[1] and the Artificial Intelligence Act (AI Act)[2] force entrepreneurs to channel precious time and capital into regulatory and legal matters. This is a marginal yet significant competitive disadvantage that compounds over time. Those two regulations in particular are constraining the creation of a grass-roots European AI sector. This may have significant repercussions, as AI is becoming a new leading sector globally, driving a new Schumpeterian growth wave. The impact of AI may be compared to the roles played by fossil-fuelled cars and the mass production of consumer goods in the late-nineteenth and early-twentieth centuries, and by information and communications technology since the 1970s.[3]

On the other hand, Big Tech poses an enormous risk to democracy and rights through its data power. This type of power is the ability to profile, manipulate and influence opinion formation through the processing of data, and then to derive actionable insights from it and operationalise them within digital environments.[4] Data power should be a key regulatory focus, as it has the potential to erode the democratic constitutional order and the individual's capacity to act as an informed citizen who can participate in the political process. The EU needs to focus on addressing the dangers of data power while clearing the way for the emergence of its AI and tech sector.

This policy brief explains how to achieve these goals through GDPR reform focused on the duty of loyalty, correlated with the significant simplification of the AI Act. The reformed GDPR should demand that data controllers or processors (entities usually processing personal data) act in the best interests of those potentially impacted (e.g. by being present in the same database or belonging to the same profile),[5] in much the same way that fiduciaries and attorneys need to act in the best interests of their clients.

1 European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L119 (4 May 2016), 1..

2 European Parliament and Council Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L1689 (12 July 2024), 1.

3 Y. Robinson and H. M. Schwartz, 'Will AI Generate a New Schumpeterian Growth Wave?', *American Affairs* 8/4 (2024); see also M. Suleyman and M. Bhaskar, *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma* (New York: Crown, 2023).

4 See O. Lynskey, 'Grappling With "Data Power": Normative Nudges From Data Protection and Privacy', *Theoretical Inquiries in Law* 20/1 (2019).

5 Note that my use here of 'data subjects' refers to all such individuals, not only those to whom data is related and who are identifiable from this data.

This is the duty of loyalty. Data processing that is not related to data power should be less regulated. This is permitted by the duty of loyalty, which should be a fulcrum of GDPR reform.

Since the duty of loyalty covers risky processing of data related to AI systems, the AI Act could be significantly simplified. The AI Act reform should be based on the repeal of obligations regarding high-risk AI systems and general-purpose AI models, while broadening and focusing both on the catalogue of prohibited AI practices and on transparency obligations.

Such a reform would simplify the regulatory framework for online entities that do not pose a significant risk to democracy and rights, thereby improving EU competitiveness and innovativeness, while also addressing the most pertinent risks, namely unchecked data power. It would render the regulatory framework more antifragile[6] in the face of ever-present technological progress and new challenges related to entities with data power. These entities include digital platforms, online gatekeepers, search engines, AI/large language models and AI ecosystem providers—and indeed, any other actor capable of accumulating significant power online.

The brief is structured as follows. The first part describes and analyses data power and argues why such power should be a focus of regulatory attention, a focus that should include determining the line that separates regulated and non-regulated entities. The gist of the argument is that data power threatens fundamental rights and their essential features, such as privacy, autonomy and hence dignity. Moreover, data power undermines the democratic constitutional order through the structural erosion of individuals' capacity to engage meaningfully in democratic life. Entities that do not pose such a risk should be either unregulated or lightly regulated and allowed to grow unless they acquire significant data power. Acceptance of the lesser risks posed by entities without data power should be traded for more economic growth, competitiveness and innovation.

The second part of the brief describes and explains the emerging corpus of EU digital law and its constitutional role in addressing the issue of data power. It focuses on (1) the GDPR as the foundational regulation for data processing—an underlying source of power online; (2) the AI Act—a key set of rules for autonomous systems, able to automatically decide on matters that are important for everyday life; (3) the Digital Services Act (DSA)—the regulation setting the rules for governing liability for online content; and (4) the Digital Markets Act (DMA)—an anti-monopoly regulation providing fair access to platforms for businesses. I treat the DSA and DMA as examples of regulations that correctly focus on entities with data power, leaving other entities with a much lower regulatory burden.

[6] Antifragile means something that benefits from disorder and change. See N. N. Taleb, *Antifragile: Things That Gain From Disorder* (New York: Random House, 2012).

The third part of the brief proposes and explains ideas that should guide the GDPR and AI Act reforms, focusing on addressing data power while allowing for increased competitiveness and economic growth. I argue that *GDPR reform should focus on the scalable, proportional and risk-based duty of loyalty towards those whose data is processed, including the obligation to refrain from exploiting their vulnerabilities*. In contrast, the AI Act reform should aim at simplification through categorical rules, such as those on prohibited AI practices and transparency duties. The AI Act should entirely remove the governance regime applicable to high-risk AI systems and general-purpose AI models. This regime creates a disproportional burden; and in any case, a reformed GDPR would address the gravest risk the current regime intends to address.

Data power: a constitutional threat that has to be reckoned with

Data power is the ability of certain entities to profile,[7] manipulate[8] and impact the opinion formation and actions of people online through control over (1) data, (2) AI systems and (3) platforms as ecosystems (understood both as software and as hardware) in which people mainly act online.[9] It is a combination of these three factors that gives rise to data power.

Profiling refers to the ability to categorise and group people in datasets based on their traits, as inferred on the basis of data mining and pattern recognition via AI systems. Profiling enables the prediction of behaviour, with an exactitude that is proportional to the quality and quantity of data, as well as the sophistication of the AI system used. The ability to create and own complex profiles of many people, if connected to control over digital environments such as online platforms or search engines, enables the display of content tailored to a profiled person. This, in turn, can influence the opinions the person forms, allowing for the potential manipulation of people. Data power is connected to ownership of the environments through which people interact. The design of such environments determines the nature of the interactions and experiences online.

7 See M. Hildebrandt and S. Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Dordrecht: Springer, 2008).

8 See R. H. Thaler and C. R. Sunstein, *Nudge: Improving Decisions About Health, Wealth, and Happiness* (London: Penguin Books, 2009).

9 Ibid., 4.

Data power encompasses a salient feature of what scholars call 'surveillance'[10] or 'informational capitalism'.[11] These terms describe a political economy in which digital platforms are the primary venue for online interaction. The user and their time and attention are the key economic resources for which entities compete online.[12] Seemingly free products and services are paid for with the user's attention and time spent on the platform. Users and their time and attention are products marketed to companies that purchase advertisements targeted at the very same profiled users.

The logic behind the attention economy can be conceptualised by using the idea of a predictive token.[13] The notion resembles 'dark patterns': interfaces devised to manipulate user choice.[14] But instead of involving design choices, a predictive token is an abstraction that signifies a broader scope of activities driving the logic of the data-intensive platform economy and data power.

A predictive token comprises (1) a computed likelihood that a target action will occur, (2) a choice-architecture change engineered to heighten that likelihood and (3) a symbolic prompt (content) that steers the individual towards the act. Predictive tokens are created when AI systems fuse personal and situational data, compare them with an individual's history and cohorts of statistically similar users, and identify the conditions most likely to trigger the intended response. The result—whether an advertisement, an interface micro-adjustment or an ambient cue—may be direct (e.g. a mood-matched advertisement seeking an instant purchase) or indirect (e.g. subtle friction that quietly prolongs a session). In either case, the online environment is primarily engineered to extend engagement, capture attention and optimise the profits derived from the increased time spent by users interacting with a platform and its advertisements.

Examples of the use of predictive tokens include (1) a social-media news feed that, drawing on prior behaviour, displays items most likely to keep the user scrolling; (2) a political campaign pinpointing swing voters and serving them tailored advertisements that covertly tilt their preferences; (3) a bank nudging customers towards behaviours its shareholders deem prerequisite for extending credit; and (4) an authoritarian state tracking dissidents and censoring activity that contravenes official dictates.

---

10 For the theory of surveillance capitalism see S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (London: Profile Books, 2019).

11 For a description of the legal construction on which informational capitalism rests, see J. E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019).

12 For a description of the attention economy and related ethical issues, see V. R. Bhargava and M. Velasquez, 'Ethics of the Attention Economy: The Problem of Social Media Addiction', *Business Ethics Quarterly* 31/3 (2021), 321.

13 J. Czarnocki, 'Containing Predictive Tokens in the EU' [Video], *IEA de Paris*, 23 May 2023.

14 See Organisation for Economic Co-operation and Development, *Dark Commercial Patterns,* Policy Paper, OECD Digital Economy Papers no. 336 (Paris: OECD Publishing, 2022).

After deployment, system controllers observe whether the user acts in line with the inducement. Deviations become fresh input, creating a refined predictive token, which is then displayed in a feedback loop—discipline and punishment by iterative nudging—until a version successfully elicits the behaviour aligned with the controllers' objectives, thereby diminishing uncertainty about future actions. In this way, online environments structurally encourage users to spend more time on the platform.

What such a predictive infrastructure yields is a probabilistic inference. Yet the unrestrained presentation of predictive tokens pushes individuals into behavioural loops that are optimal for the owners of the digital environments. In extreme scenarios, people may find themselves effectively bound by their data-fied pasts, with limited space for change and even impelled to intensify existing patterns, posing grave threats to privacy and personal autonomy. The owners of digital environments are thus incentivised to cater to the lowest instincts that data analytics can discover in each of us and to double down on them, capturing the dopamine-driven circuits through the display of content that incites extreme emotions and thus prolongs attention to the platform. Anyone can quickly test this assertion by using TikTok for an hour—surely spiritual elation is a relatively rare occurrence after prolonged use.

The bottom line is that the majority of digital business models rely on engagement, attention capture and optimisation. The revenue generated is directly proportional to the attention paid by users and the time they spend—and the time spent relates to the emotions elicited during use (both positive and negative). Therefore, online environments, powered by AI algorithms, are structurally designed to be addictive.

Online environments not only impact our opinions and decisions but also structurally erode our cognitive abilities and contribute to social isolation, fragmentation and depression.[15] The creation of increasingly fragmented opinion bubbles, moreover, erodes political consensus and a narrative that people hold in common, which is essential for a functioning democracy. Furthermore, controllers of online environments are not incentivised to share content that contradicts an implicit or explicit bias, to expose users to a contrary point of view, as it may diminish the time and attention devoted to that environment. However, engagement with differing points of view is the essence of democracy, public discourse and rational deliberation—all preconditions for the very existence of the democratic constitutional order.[16]

The economic logic driving most of the profit pursued by major entities is inherently against the ideal of an informed, rational and engaged citizen, an ideal which is indispensable

[15] See J. Haidt, *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (New York: Random House, 2024).

[16] The ability to rationally communicate and deliberate is a precondition for the modern theory of liberal democracy, as presented by Habermas: J. Habermas, *The Theory of Communicative Action, vol. 1: Reason and the Rationalization of Society*, trans. T. McCarthy (Boston: Beacon Press, 1985).

for the existence of democracy. Therefore, data power poses a threat to democracy and people's constitutional rights.

In turn, also worrying is that although the primary incentive driving data power is profit, such power, once accumulated, is easily translatable into an illegitimate and democratically unaccountable political power. Entities with data power accrue more and more illegitimate power, unchecked by the democratic process and institutions, at the expense of increasingly disempowered and cognitively confused citizens. This process keeps on eroding the very pillars on which a democratic society and state are constituted. This threat needs to be addressed accordingly. Therefore, it is imperative to create a regulatory environment that strikes a balance between the manifold benefits stemming from the digitalisation and development of the infosphere and the structural risks inherent in what enables profit to be made in this realm.

EU digital law—an answer to the constitutional threat of data power to democracy

The challenges mentioned above are the subject of a rich body of interdisciplinary scholarship, including that on digital law. The reason for separating digital law (previously known as cyberlaw) from other branches of legal studies was the factual, qualitative and quantitative difference in the degree to which one party can directly impact the behaviour of another online as compared to in an offline, real-world setting.[17] What sets online experiences apart from offline ones is that the former are entirely orchestrated by digital infrastructure and code, which creates a set of altogether different affordances[18] for those providing online experiences on the one hand, and those using these experiences on the other.

The providers of online experiences have asymmetrical control over these experiences, while users need to adjust their behaviour to the way the online environment is orchestrated through code. For instance, in the real or analogue world, while the reader sits and reads this text, it is unlikely that the architect, builder or administrator of the building in which the reader resides will enter the room and observe what the reader is doing at this moment. This is not the case online. In principle, those who control online environments

[17] L. Lessig, 'The Law of the Horse: What Cyber Law Might Teach', *Harvard Law Review* 113/2 (1999), 501.

[18] Affordances in ecological psychology are what the environment offers a human or an animal, what it provides or furnishes, either for good or ill. It refers to possibilities of action provided by the environment, relative to the capabilities and needs of a specific organism. See J. J. Gibson, 'The Theory of Affordances', in R. Shaw and J. Bransford (eds.), *Perceiving, Acting, and Knowing: Toward an Ecological Psychology* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1977), 67.

can access readers' data at any time; monitor their activities (breaching privacy); and then, for example, delete these data, conceal them or algorithmically deprioritise them (violating freedom of speech).

The EU is very active in addressing the threats posed by data power, via the emerging corpus of EU digital law.[19] Arguably, the most impactful among these laws are (1) the GDPR—regulating flows of personal data; (2) the DSA[20]—regulating responsibility for content and intermediary services online; (3) the DMA[21]—regulating access to data and to the platform economy; and finally, (4) the AI Act—regulating the development and placing of AI systems in the EU single market.

The GDPR regulates and governs the processing of personal data.[22] This is data that enables the identification of a person: in simple terms, it means the ability to distinguish someone from the crowd, thus denying anonymity. The purpose of the GDPR is both to protect fundamental rights to privacy and data protection, and to facilitate free flows of data within the EU single market.[23] The GDPR demands that personal data be processed on a lawful basis,[24] which can be interpreted as having a legally recognised and legitimising reason for processing, such as consent, contractual necessity or legitimate interest. The GDPR also requires that personal data is always processed in accordance with data protection principles.[25] These principles have various functions, including to limit the allowed scope and amount of data processing to what is necessary to achieve the purpose of processing and to restrict the storage of data to what is necessary to accomplish this purpose. Personal data must also be processed securely and transparently. Moreover, those who process personal data are accountable and can be held liable through data rights, which are granted to those whose data is processed. Furthermore, supervisory authorities are empowered to impose fines for illegal processing.

The DSA governs the liability of entities intermediating content provision online. Examples of such entities are online platforms, including very large online platforms such as X (Twitter), TikTok and Facebook.[26] The DSA limits the liability of the intermediary platform for the content, provided it complies with the laws of the given EU member state regarding

---

19 For an overview of the term, see J. Czarnocki and P. Palka (eds.), *Proportionality in EU Digital Law: Balancing Conflicting Rights and Interests* (London: Bloomsbury Publishing, 2024).

20 European Parliament and Council Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act), OJ L277 (27 October 2022), 1.

21 European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L265 (12 October 2022), 1.

22 Art. 2 of the GDPR.

23 Art. 1 of the GDPR.

24 Art. 6 of the GDPR.

25 Art. 5 of the GDPR.

26 European Commission, 'Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines', Press Release (Brussels, 24 April 2023).

illegal content and the specific due diligence rules outlined in the DSA. This means that platforms are not liable for the content uploaded by users. However, platforms need to establish clear and transparent rules of content governance and allow for an appeal process for content takedown decisions. They also need to establish an auditable governance structure that provides insight into their algorithmic processes that govern the provision of content. Importantly, the DSA prohibits the profiling of children.[27] It also prohibits the use of dark patterns,[28] thereby addressing an essential aspect of data power.

The DMA is a governance framework designed to promote fair competition online by regulating the conditions under which marketplaces share data with other entities that transact through them. The DMA also prohibits entities from engaging in activities that would diminish the ability of other entities on the marketplace to effectively compete.[29] The DMA regulates the activities of gatekeepers and of the entities providing core platform services (such as marketplaces and app stores), online search engines, social networks, video-sharing platforms, interpersonal communication services, operating systems, web browsers, virtual assistants, cloud-computing services and online advertising services (including advertisement intermediation).[30] In this way, the DMA aims to limit the market power of certain online entities. Through its pro-competitiveness, it limits data power by providing a possibility for the growth of product and service providers offering alternatives to players with entrenched positions. What is also significant is that the DMA prohibits the merging of personal data streams from different platforms, unless a person has given their consent.[31] This also potentially limits data power.

The AI Act regulates the placement of AI systems on the EU single market, with a focus on high-risk and general-purpose AI. It also prohibits specific AI systems, such as facial recognition (with exclusions for national security-related use[32]), and facilitates transparency rules for generative AI that creates, for example, deepfakes and other types of synthetic content. The regulatory focus of the AI Act is on systems that pose a high risk to fundamental rights and on general-purpose AI models. For these types of AI, the AI Act mandates the establishment of comprehensive compliance and risk-management processes that should, in a transparent and accountable manner, minimise the risks to fundamental rights.

27 Art. 28(2) of the DSA.

28 Arts.. 25(1) of the DSA.

29 Art. 5, 6 and 7 of the DMA.

30 Art. 2(2) of the DMA.

31 Art. 5(2) of the DMA.

32 Art. 5(1) and (2) of the AI Act.

All of the above-mentioned regulations rely to a great extent on the proportionality principle[33] and a risk-based approach.[34] Proportionality is a general principle of EU law[35] that demands that any limitation to a right is necessary and suitable and that its benefits outweigh the potential detriment. In a broader legal sense, proportionality refers to adjusting measures to meet the regulatory or compliance requirements of the context in which the law is applied. In this way, proportionality relates to the risk-based approach that underpins all the laws mentioned above.[36] A risk-based approach means that the precise way in which regulatory requirements are fulfilled needs to be adjusted to the actual risk present in a given context. For example, this means that the GDPR, when demanding security of personal data, implicitly requires a different and higher level of compliance from a bank compared to an online e-commerce platform. Both as a principle and as a risk-based approach, proportionality provides a certain scope of elasticity in how regulated entities fulfil their duties. Both proportionality and risk-based approaches are important, as they represent an imperative for legal principles and rules to be adjusted to the degree and likelihood of risk—for example, the risk to rights.

What all these laws have already achieved is laudable. The GDPR introduced a comprehensive governance model for limiting risks related to personal data processing. Regulations that followed, such as the DSA and DMA, introduced clear-cut rules addressing data protection (supplementing the GDPR rules), including prohibitions on profiling children or profiling with the use of special categories of personal data, as outlined in the DSA. Most recently, the AI Act filled another gap by outlawing certain prohibitively risky AI systems, such as facial recognition.

However, many of the regulations comprising this new legal system are disproportionate.[37] Suppose the DSA and DMA correctly recognise entities with data power and regulate them accordingly. In that case, the GDPR and AI Act apply, respectively, whenever the personal data of an EU citizen is processed or an AI system poses a risk that is not negligible (according to this law). However, the GDPR and AI Act are too broad in scope. These two regulations are also very complex, creating an elevated compliance burden for EU competitiveness and innovation. They unduly disadvantage entities that do not pose a tangible risk to the rights of EU citizens or democracy because the amount of data over which these entities have control is limited, as is the possibility of using these data through harmful and risky AI systems or platform ecosystems.

---

33 Ibid., footnote no. 15.

34 See G. De Gregorio and P. Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age', *Common Market Law Review* 59/2 (2022).

35 Art. 52 of the Charter of Fundamental Rights of the European Union, OJ C326 (26 October 2012), 391.

36 De Gregorio and Dunn, 'The European Risk-Based Approaches', footnote no. 36.

37 See, for instance, P. Palka, 'Proportionality of Goals or Means? The Politics of Data Governance in the Shade of Constitutional Norms', in J. Czarnocki and P. Palka (eds.), *Proportionality in EU Digital Law: Balancing Conflicting Rights and Interests* (London: Bloomsbury Publishing, 2024).

The GDPR and AI Act create prohibitive entry barriers and operational burdens for new players entering the market. These regulations create a chilling effect on industriousness, entrepreneurship and innovation by creating an administrative burden and additional operational costs. These two regulations shift the attention of entrepreneurs away from competing and innovating to addressing risks related to compliance and the related costs. Unburdened by similar regulatory demands, new players in other jurisdictions move faster than EU companies, outcompeting and outperforming them. Additionally, EU entrepreneurs themselves relocate to these jurisdictions, initially focusing on markets where such burdens do not exist. Paradoxically, these laws may also favour large players, which can afford the costly and operationally demanding compliance. This is because such players already possess sufficient financial, technical and organisational acumen to comply, without, however, having their data power substantially constrained.

Recommendations for GDPR and AI Act reform: a focus on data relationships and the duty of loyalty

It is necessary, therefore, to design a regulatory solution that can reform the GDPR and AI Act in a way that preserves and enhances their ability to address data power while significantly reducing the burden on entities that do not pose a significant risk. This new solution should be scalable in proportion to the risk, in line with a risk-based approach. It should also accommodate the lowering of complexity by reducing the number of rules. The number of articles and recitals in the GDPR and AI Act is, in itself, a challenge to comprehensibility and certainty of legal interpretation.

In general, the GDPR assumes that the protection of privacy and personal data is best achieved through the uniform application of rules to entities that process personal data. It also assumes that a massive chain of fairly transparent contractual relationships, facilitated through data protection agreements and disclosures of subprocessors, is an effective way to protect personal data.[38] The GDPR forces any parties processing or sharing personal data to secure their protection through the systems of contracts that govern subprocessing and data transfers.[39] At some point, however, the relationship between those from whom personal data are collected and those who process the data is severed. This means that the context is lost, and it is impossible for the processor to substantially comply. That is because substantial compliance with the GDPR depends on the knowledge of a particular (usually the first) act of processing, when personal

[38] Chapter IV of the GDPR.

[39] Chapter V of the GDPR.

data is collected, and the application of rules in this given context. It follows that, for the majority of subprocessing, knowledge of the initial context of processing is lost. What remains is an uninformed, superficial application of rules by subprocessors, which lack the initial context of personal data processing.

Moreover, the current interpretation of the GDPR emphasises consent as a primary safeguard of rights to privacy and data protection. In many commercial instances, personal data must not be processed unless consent is obtained[40] or an appropriate contract necessitating processing is in place.[41] The effectiveness of consent, however, is dubious and widely criticised, both in the EU[42] and the US.[43] Although the procedure can be complied with, people often do not know what they are consenting to. That is because it is impossible to reasonably anticipate how personal data will be processed downstream in complex processing environments, such as those of the Big Tech giants. Additionally, reliance on contractual regimes between the parties processing data and the individuals whose data is processed glosses over significant informational and power asymmetries. Such an approach to data protection also ignores the group impact of personal data processing. Given the nature of data mining and derivable insights, an individual's personal data enriches a database, the impact of which is not confined to that individual—data provided by that individual aids in profiling and targeting other people.[44] This often renders consent and accompanying contracts hollow as proper safeguards.

Legitimate interest is another legal basis for processing.[45] However, at this point, the GDPR offers limited scope for protection, as those who process data are not required to disclose how they assess the balance of rights and interests when they decide to process personal data. That is, entities that process personal data do not have to demonstrate how they neutralise their own asymmetrical advantages related to processing to make it legal. Therefore, the power dimension of personal data processing is effectively neglected in the GDPR. This means that the nature of the relationship between the entities that process personal data and those whose data is processed is not a central dimension impacting the scope of protection.

40 Art. 7 of the GDPR.

41 Art. 6(1)(b) of the GDPR.

42 Lynskey provides an up-to-date overview of the problems related to consent, in the broader perspective of the GDPR's role in EU digital law. See O. Lynskey, 'Complete and Effective Data Protection', *Current Legal Problems*, 76/1 (2023).

43 See D. J. Solove, 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review* 126/7 (2013), and D. J. Solove, 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law', *Boston University Law Review* 104/2 (2024).

44 See L. Taylor, L. Floridi and B. van der Sloot (eds.), *Group Privacy: New Challenges of Data Technologies* (Cham: Springer, 2017).

45 Art. 6(1)(f) of the GDPR.

However, there are hints in the text of the GDPR that the nature of the relationship—including the amount of power wielded by the different parties—should be an evaluative criterion.[46] In practice, this issue is often overlooked. Even in a world where the parties processing data diligently disclose their methods and means of processing personal data, it is challenging to anticipate what will happen to the data and what detrimental consequences may arise. Yet, the GDPR assumes there is knowledge parity between the data subject and the data controller or processor and that, if information is transparently disclosed, giving consent or signing a contract legitimises the processing.

Against this tendency, the relationship between data controllers and processors and data subjects should become a central regulatory focus, around which the protection of personal data should be orchestrated. When personal data is processed, it is the nature of the relationship that should determine the proportional and risk-based duties that data controllers and processors have towards data subjects. Instead of highly procedural rules governing all personal data processing, the focus should be on what is possible in the given context, as well as on the actual threats to rights and democracy, given the particular context of processing. This would mean that entities that process personal data would need to refrain from actions that threaten the best interests of data subjects. This is the duty of loyalty as conceived by Richards and Harzog for US privacy law reform.[47] The Continental legal analogue of this concept can be found in the principle of good faith (bona fide), yet the US legal framing makes it better suited to fiduciary relationships.

Richards and Hartzog set forth their concept of the duty of loyalty by contrasting it with the 'consent and notice' paradigm, which means treating the consent of an individual as authorisation for any processing of personal data, as long as it is disclosed in lengthy and opaque privacy notices and policies (to which users automatically consent whenever they use a new service online). It is true that the GDPR's rule set for protecting privacy through the protection of personal data is more comprehensive than the US 'consent and notice' paradigm. However, various deficiencies of this paradigm have still not been alleviated by the GDPR. Therefore, Richards and Hartzog's ideas could also be applied to inspire the reform in the EU.

The main shortcoming of the GDPR, as currently interpreted, is that it is oblivious to the power imbalance and type of relationship between data controllers or processors and data subjects. It is not explicitly concerned with the vulnerability of a person related to personal

46 Recital 47 of the GDPR.

47 See the arguments presented by these authors in the following series of articles: N. Richards and W. Hartzog, 'A Duty of Loyalty for Privacy Law', *Washington University Law Review* 99 (2021); N. Richards and W. Hartzog, 'A Relational Turn for Data Protection', *European Data Protection Law Review* 6/4 (2020); N. Richards and W. Hartzog, 'Taking Trust Seriously in Privacy Law', *Stanford Technology Law Review* 19 (2016); N. Richards and W. Hartzog, 'The Surprising Virtues of Data Loyalty', *Emory Law Journal* 71/5 (2022).

data disclosure.[48] Against this backdrop, the duty of loyalty implies that whenever personal data is processed, a trust relationship is established (the fiduciary principle) between data controllers or processors and data subjects. Trust means that one feels a sense of security in relation to a party to whom one is vulnerable or who could cause one harm.[49]

Such a duty has its source in the trust people confer when they disclose their data, and in people's vulnerability when their data is harvested without their knowledge or consent. Trust is inseparable from vulnerability: trust means making oneself vulnerable to another party by, for example, exposing sensitive information, with the anticipation that this trusted party will not exploit this vulnerability. Personal data processing creates a relationship of trust because it discloses knowledge about either the individual or other people associated with him or her through commonly held traits. Such processing creates conditions in which vulnerabilities that have been exposed, via the processed data, can be exploited against the interests of the people concerned.[50]

In the context of the processing of personal data, loyalty means that at any stage of the processing, the party processing the data must act in the best interests of the data subjects, or others who may be impacted by the processing, even if their data is not directly processed.[51] The duty of loyalty would create a prohibition against exploiting vulnerabilities that arise when data is processed and managed. It would also require data controllers and processors to consider the actual interests of those impacted and then that these entities be held to account for how they make their assessments of such interests. In this way, many predatory data power practices could be outlawed, because the duty of loyalty would force lawmakers, courts and supervisory authorities to take a stance on how the processing of data betrays people's trust.

Such loyalty, moreover, could mean entirely different things in the context of, for example, financial services, banking and insurance on the one hand, and medical services on the other, and yet different things in the context of search engines, news feeds and other social media. A one-size-fits-all solution no longer applies. Yet, regardless of the industry, '[l]oyalty would demand that organizations refrain from design choices that foreseeably extract data, labor, or attention from trusting parties or prey on trusting parties' limited resources or cognition for coercive purposes that conflict with a trusting party's best interests.'[52]

---

48 Malgieri discusses the vulnerability related to disclosing personal data in his monograph, proposing an interpretative framework within the current GDPR. Yet, I argue that such a framework is only feasible for a knowledgeable legal scholar, not an everyday lawyer, and least of all a layman. See G. Malgieri, *Vulnerability and Data Protection Law* (Oxford: Oxford University Press, 2023).

49 Ibid.

50 This is one of the main arguments presented by Malgieri in *Vulnerability and Data Protection Law*.

51 This may also require a redefinition of what types of data are regulated, broadening the scope beyond personal data. But such a discussion is beyond the scope of this policy brief.

52 Richards and Hartzog, 'The Surprising Virtues of Data Loyalty'.

Such a new, loyalty-based GDPR could demand more substantial and context-dependent compliance,[53] focusing on its effects rather than procedural appropriateness and compliance, as it does currently. Scholars who advocate such an approach argue that '[n]ot only does a duty of loyalty offer substantive protections that a GDPR-style approach does not but that loyalty can also offer political and moral salience to rules that restrain the uses of human information that European data protection terms such as "data minimization" and "legitimate interest" simply cannot.'[54]

In effect, such an approach forces transparency and accountability because it does not predetermine what information is to be disclosed and explained, but demands that (1) disclosures be made and explanations be given in connection with any meaningful information and (2) evidence be given that proves that parties processing data are acting in the best interests of the data subject—or at least that these parties are refraining from abuse and harm. In this way, introducing the duty of loyalty and perceiving the GDPR as a matter of trust and balanced relationships would make it much easier to determine clear red lines and identify practices should be are outlawed because they exploit people's vulnerabilities and abuse their trust. This would most likely leave most entities unregulated or lightly regulated, if they pose a negligible risk. Here, the level of data power could serve as an analytical benchmark, determining whether data processing is risky or not. As Richards and Hartzog point out, 'The more power a company has in a relationship, the more protective and loyal it must be.'[55]

In practice, GDPR reform should focus on the duty of loyalty, which means that whenever a data controller or processor processes data and such processing could impact people, it should assess what acting in their best interests means. Practically speaking, it means that the GDPR's data protection principles[56]—such as purpose limitation, storage limitation, data minimisation, security and accuracy—would be normative guides to inform the substantive interpretation of the duty of loyalty in specific cases. What would change, as well, is that an elaborate contractual regime between subprocessors would no longer be required, as any entity processing data with the likelihood of impacting EU citizens would by default be subject to the new GDPR and the duty of loyalty, and to obligations to act in the best interests of those EU citizens who may be impacted.

In practice, such an approach would mean that the GDPR should be reframed around the duties that any party has when it processes personal data. However, such duties should not be perceived as obligations to the data subjects whose data a particular

---

53 See the importance of context for privacy in the contextual theory of privacy presented in H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010).

54 Richards and Hartzog, 'The Surprising Virtues of Data Loyalty', 990.

55 Ibid.', 995.

56 Art. 5 of the GDPR.

data controller or processor has but rather to the general public and anyone likely to be impacted by a data controller's or processor's processing.

With such an approach, compliance moves from being a game of enlisting compliance measures and arcane interpretations of procedural terminology—without due regard for the underlying substantial risks of personal data processing—to being a process of substantial legal and contextual argumentation regarding what is legally and morally right and wrong in the digital world. And the question of what is right is one we need to keep asking ourselves, given the relentlessness of the progress in the digital economy and the tendencies towards monopolisation and data power accumulation. In practice, the duty of loyalty would mean that each data controller or processor processing data that impacts people would need to meaningfully assess the context of processing, the potential power the data holds and what it means to act in the best interests of the people whose trust it has in that context.

Such an approach could align with the proportionality principle and risk-based approach. The more capacity the party has for processing data, the higher the risk and the more stringent the safeguards that should be implemented to protect data (and privacy). The focus should not be on arguing about whether this or that measure is appropriate or whether data is protected well (this line of reasoning assumes that the most significant risk is a potential data breach). Instead, it should be asked whether a party processing data is acting in the best interests, or at least not against the interests, of those whose data is being processed.

If such a reform of the GDPR is conducted, then the AI Act could be simplified. The EU should repeal duties related to high-risk AI systems and general-purpose AI models while keeping and perhaps broadening the catalogue of prohibited AI practices[57] and transparency obligations[58] as key substantial requirements governing AI systems. The reason is that the GDPR reform described could have results similar to those purportedly achieved by the regulations on high-risk AI systems and general-purpose AI models. That is because any process of AI system research and development entails the processing of personal data and thus demands substantial compliance with the duty of loyalty and all that it entails. Moreover, as deployers of AI systems would already be subject to the new GDPR, through which the duty of loyalty would limit what the AI Act aims to limit—that is, risks to fundamental rights—the AI Act could be simplified in the following way. Together with the GDPR reform proposed above, the AI Act could be changed so that if an AI system that has not been trained using EU citizens' personal data is to be deployed in the EU, the duty of loyalty applies to the data that was used, in terms of the actual impact such data has in the EU.

57 Art. 5 of the AI Act.

58 Art. 50 of the AI Act.

This approach is future-proof, antifragile and elastic enough to keep pace with new technological methods, such as large language models or AI agents. That is because it provides a broader scope of freedom regarding how compliance is achieved in relation to the intended effect: through acting in the interests of those whose data is processed, rather than merely verifying whether the rules have been followed, regardless of the outcome. It encompasses any future risks that the further development of digital technologies may create, as it maintains a focus on the relationship between data controllers or processors and data subjects. In this way, this approach does not overlook the possibility of novel data processing methods.

Recommendations for GDPR and AI Act reform

The following recommendations outline a clear direction for reform. It must be emphasised, however, that the precise operationalisation of these ideas deserves more extensive study and careful reflection to secure full coherence and consistency in the final legal architecture. The primary objective is to more effectively address the constitutional threat of data power by focusing regulatory scrutiny on the entities capable of wielding it. This targeted approach allows for a significant simplification of the legal framework, reducing the compliance burden for startups and other entities that do not pose a tangible risk to rights and democracy, thereby boosting EU competitiveness. Concurrently, by anchoring the reform in the scalable duty of loyalty, the aim is to create a more future-proof and antifragile digital law that can adapt. Finally, these changes seek to foster a legal environment that prioritises comprehensible, substantive yet proportional and risk-based compliance over procedural window dressing.

Proposed changes to the GDPR

1. *Introduce the duty of loyalty.* Amend the GDPR to insert a new core principle establishing this obligation. This would legally require any entity processing personal data to act in the best interests of the people potentially affected by that processing and to refrain from exploiting their vulnerabilities. This duty would serve as the primary interpretive guide for the entire regulation.

2. *Define 'data power' and establish a rebuttable presumption.* Introduce into the GDPR a legal definition of 'data power', conceptualised as the capacity to profile, manipulate and influence the behaviour of a significant number of people through the combined control of data, AI systems and digital ecosystems. Establish a rebuttable presumption that a data controller or processor (but also any other entity

processing data) possesses significant data power—and is thus subject to the highest level of the duty of loyalty—if it meets one or more of the following criteria:

- It is designated as a Very Large Online Platform or Very Large Online Search Engine under the DSA.
- It is designated as a 'gatekeeper' of a core platform service under the DMA.
- It provides or deploys (1) a 'high-risk AI system' (as defined by the AI Act) at a significant scale within the EU market (assuming no change of the AI Act) or (2) other automated decision-making AI systems which significantly impact people's rights and life prospects.

3. *Solidify extraterritorial application*. On top of the already existing scope, the GDPR must apply to any entity accepting transfers of and processing the personal data of EU citizens, regardless of where that entity is located or whether a direct contractual relationship exists. The obligation attaches to the data itself. The acceptance of EU citizens' personal data, especially by a subprocessing entity, means that that entity is subject to the GDPR. This eliminates loopholes in complex data processing chains and ensures that the duty of loyalty directly binds any subprocessor.

4. *Repeal mandatory contractual duties between controllers and processors*. The elaborate and often merely formal requirements of Article 28 (controller–processor contracts) would become redundant. If any entity processing EU citizens' personal data is directly bound by the duty of loyalty as it accepts the transfer of this personal data, the need for a complex chain of contractual liability is significantly reduced, simplifying compliance for the entire ecosystem.

5. *Strengthen legitimate interest and create an integrated data protection assessment.* Consent and contract (contractual necessity) should no longer be the primary gateways for processing. Instead, they should be reserved for situations in which there is genuine doubt as to whether a processing activity aligns with a person's best interests and whether there is a proper balance in the relationship. Thus, Article 6 of the GDPR should establish legitimate interest as the primary legal basis for data processing. The associated proportionality balancing test must be transformed into a mandatory, documented and substantive assessment of how the processing aligns with the duty of loyalty and of the risks that arise in view of this duty. Such an assessment would have to be disclosed to the public (e.g. via a privacy policy or another appropriate medium) if a controller was a data power controller. The majority of the documentation requirements should be reduced and folded into such an overarching assessment (e.g. a record of processing activities and a data protection impact assessment).

6. *Redefine core principles in terms of the basic concept of loyalty.* Amend Article 5 of the GDPR to reinterpret key principles so that loyalty becomes the foundational idea. 'Fairness' would be explicitly defined as the non-exploitation of vulnerabilities, while 'transparency' would require the meaningful disclosure of power asymmetries and the foreseeable impacts of processing.

7. *Shift from a contractual to a public relationship model*. A controller's duties should be conceptualised as owed not just to individual data subjects but to the broader public potentially affected by the controller's data operations. This model recognises that data power may cause societal harm (e.g. democratic erosion and opinion fragmentation) that goes beyond personal risks to the individual.

8. *Link obligations to scope and risk*. The intensity of the duty of loyalty must be proportional to the controller's data power. An integrated assessment should be used to gauge the controller's capacity to profile and influence at scale. Entities with no or negligible data power would have lighter, more manageable obligations while those with significant data power would face stringent requirements.

9. *Establish sector-specific guidelines and codes of practice*. Enhance Article 40 (on codes of conduct) to create a formal mechanism for developing and approving sector-specific guidelines. These codes, created in collaboration with industry stakeholders and supervisory authorities, would translate the abstract duty of loyalty into concrete, actionable requirements for specific industries (e.g. finance, healthcare and social media). Adherence to an approved code would create a rebuttable presumption of compliance, providing legal certainty and clear standards based on the specific risks and scope of the processing involved. For startups and small and medium-sized enterprises, except for an integrated assessment as proposed above, compliance with established, high-quality industry standards (e.g. ISO/IEC 27001 or SOC 2 Type II) could create a rebuttable presumption of compliance with the technical and organisational aspects of the duty of loyalty, providing a clear and achievable benchmark.

Proposed changes to the AI Act

1. *Repeal rules applying to high-risk AI systems and to general-purpose AI systems and models in the AI Act*. Repeal Chapters III and V of the AI Act , which detail the complex classification, conformity assessment, and governance obligations for high-risk AI systems and general-purpose AI models. A reformed, loyalty-based GDPR would substantively address the underlying risks to fundamental rights, making these parallel structures redundant.

2. *Develop the catalogue of prohibited practices to cover more of these activities*. Retain and strengthen Article 5 of the AI Act as the core of the regulation. The list of prohibitions should be expanded from banning specific technical methods to

outlawing AI systems based on their harmful effects, such as those designed to exploit known cognitive biases or create manipulative behavioural loops contrary to a person's best interests.

3. *Strengthen and simplify transparency duties in Chapter IV of the AI Act*. Refocus transparency obligations away from box-ticking compliance towards meaningful public disclosure. This would include mandating clear, plain-language declarations about the use of AI for persuasive or behaviour-steering purposes and ensuring that all synthetic media are clearly and permanently identifiable.

Conclusion

This policy brief has advanced four connected claims. First, data power—the combined control of massive amounts of data, predictive systems and user environments—poses a structural threat to privacy, autonomy and the democratic order. Proportionate and risk-based regulation needs to distinguish actors able to wield that power from those that cannot. Second, current EU digital law only partially achieves this goal. The DSA and the DMA target entities with significant data power, yet the GDPR and the AI Act apply the same stringent scheme to the entire market. This can dampen the efforts of smaller innovators and produce ambiguity due to the size and complexity of these regulations. Third, the remedy is to anchor the GDPR in the duty of loyalty, which focuses on the nature of the relationship between those who process data and those whose data is processed. When entities must act in the best interests of the people they affect, protection becomes proportional to real power relationships. Fourth, a GDPR that is focused on the duty of loyalty would make way for a leaner AI Act. This means maintaining the catalogue of prohibited practices and transparency duties but repealing the complex governance regime for high-risk and general-purpose AI since the related concerns would be addressed by duty-of-loyalty data processing.

However, it needs to be emphasised that the precise way the duty of loyalty should be operationalised deserves much more extensive study, as does the question of exactly how the reforms of the GDPR and the AI Act should be conducted. This brief is aimed at focusing the attention of regulators on the challenge of data power and at proposing an emphasis on data-based relationships and the associated trust and loyalty as key drivers of meaningful change. Such a change would mean, first, a more balanced relationship between those who process data and those whose data is processed; and second, a lighter regulatory burden when the risks to rights and democracy are limited. There is no need to constrain competitiveness and innovation.

Taken together, these changes could realign EU digital law both to better guard rights and to improve competitiveness. Entities lacking significant data power would face lighter

obligations, while entities with greater data power would have to contend with more stringent obligations. By shifting the focus from procedures to relationships when data is processed, the EU could better mitigate the constitutional risks of data power without compromising competitiveness.

Bibliography

EU legislation

Charter of Fundamental Rights of the European Union, OJ C326 (26 October 2012), 391, accessed at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2012:326:TOC on 17 September 2024.

European Parliament and Council Regulation (EU) 2016/679 on the protection of natural persons about the processing of personal data and on the free movement of such data (General Data Protection Regulation), OJ L119 (4 May 2016), 1, accessed at https://eur-lex.europa.eu/eli/reg/2016/679/oj on 18 June 2025.

European Parliament and Council Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Act), OJ L265 (12 October 2022), 1.

European Parliament and Council Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act), OJ L277 (27 October 2022), 1.

European Parliament and Council Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L1689 (12 July 2024), 1.

Books, edited volumes and chapters

Cohen, J. E., *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford: Oxford University Press, 2019), doi:10.1093/oso/9780190246693.001.0001.

Czarnocki, J. and Palka, P. (eds.), *Proportionality in EU Digital Law: Balancing Conflicting Rights and Interests* (London: Bloomsbury Publishing, 2024).

De Gregorio, G., 'Digital Constitutionalism: An Introduction', in G. De Gregorio (ed.), *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society* (Cambridge: Cambridge University Press, 2022), 1–37.

Gibson, J. J., 'The Theory of Affordances', in R. Shaw and J. Bransford (eds.), *Perceiving, Acting, and Knowing: Toward an Ecological Psychology* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1977), 67–82.

Habermas, J., *The Theory of Communicative Action, vol. 1: Reason and the Rationalization of Society*, trans. T. McCarthy (Boston: Beacon Press, 1985).

Haidt, J., *The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness* (New York: Random House, 2024).

Hildebrandt, M. and Gutwirth, S. (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Dordrecht: Springer, 2008), doi:10.1007/978-1-4020-6914-7.

Malgieri, G., *Vulnerability and Data Protection Law* (Oxford: Oxford University Press, 2023).

Nissenbaum, H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010).

Palka, P., 'Proportionality of Goals or Means? The Politics of Data Governance in the Shade of Constitutional Norms', in J. Czarnocki and P. Palka (eds.), *Proportionality in EU Digital Law: Balancing Conflicting Rights and Interests* (London: Bloomsbury Publishing, 2024) 109–16.

Suleyman, M. and Bhaskar, M., *The Coming Wave: Technology, Power, and the Twenty-First Century's Greatest Dilemma* (New York: Crown, 2023).

Taleb, N. N., *Antifragile: Things That Gain From Disorder* (New York: Random House, 2012).

Taylor, L., Floridi, L. and van der Sloot, B. (eds.), Group Privacy: New Challenges of Data Technologies (Cham: Springer, 2017).

Thaler, R. H. and Sunstein, C. R., *Nudge: Improving Decisions About Health, Wealth, and Happiness* (London: Penguin Books, 2009).

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

Journal articles

Bhargava, V. R. and Velasquez, M., 'Ethics of the Attention Economy: The Problem of Social Media Addiction', *Business Ethics Quarterly* 31/3 (2021), 321–59, doi:10.1017/beq.2020.32

De Gregorio, G. and Dunn, P., 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age', *Common Market Law Review* 59/2 (2022), 473–500, doi:10.54648/cola2022032

Hindman, M. and Cukier, K. N., 'The Macroeconomics of Attention and Information', *Journal of Economic Perspectives* 32/2 (2018), 199–224.

Lessig, L., 'The Law of the Horse: What Cyber Law Might Teach', *Harvard Law Review* 113/2 (1999), 501–49.

Lynskey, O., 'Complete and Effective Data Protection', *Current Legal Problems* 76/1 (2023), 297–344, doi:10.1093/clp/cuad009.

Lynskey, O., 'Grappling With "Data Power": Normative Nudges From Data Protection and Privacy', *Theoretical Inquiries in Law* 20/1 (2019), 189–220, doi:10.1515/til-2019-0007.

Richards, N. and Hartzog, W., 'A Duty of Loyalty for Privacy Law', *Washington University Law Review* 99 (2021), 961–1049.

Richards, N. and Hartzog, W., 'A Relational Turn for Data Protection', *European Data Protection Law Review* 6/4 (2020), 492–97, doi:10.21552/edpl/2020/4/5.

Richards, N. and Hartzog, W., 'Taking Trust Seriously in Privacy Law', *Stanford Technology Law Review* 19 (2016), 431–71.

Richards, N. and Hartzog, W., 'The Surprising Virtues of Data Loyalty', *Emory Law Journal* 71/5 (2022), 985–1033, accessed at https://scholarlycommons.law.emory.edu/elj/vol71/iss5/4 on 18 June 2025.

Robinson, Y. and Schwartz, H. M., 'Will AI Generate a New Schumpeterian Growth Wave?', *American Affairs* 8/4 (2024), 16–32, accessed at https://americanaffairsjournal.org/2024/11/will-ai-generate-a-new-schumpeterian-growth-wave/ on 23 July 2025.

Solove, D. J., 'Murky Consent: An Approach to the Fictions of Consent in Privacy Law', *Boston University Law Review* 104/2 (2024), 593–638, doi:10.2139/ssrn.4333743.

Solove, D. J., 'Privacy Self-Management and the Consent Dilemma', *Harvard Law Review* 126/7 (2013), 1880–903, accessed at https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/ on 1 September 2025.

Reports

Organisation for Economic Co-operation and Development, *Dark Commercial Patterns*, Policy Paper, OECD Digital Economy Papers no. 336 (Paris: OECD Publishing, 2022), doi:10.1787/44f5e846-en.

EU documents and press releases

European Commission, 'Digital Services Act: Commission Designates First Set of Very Large Online Platforms and Search Engines', Press Release (Brussels, 24 April 2023), accessed at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413 on 18 June 2025.

Other sources

Czarnocki, J., 'Containing Predictive Tokens in the EU' [Video], *IEA de Paris*, 23 May 2023.

About the author

Jan Czarnocki is a doctoral researcher and Marie Skłodowska-Curie Fellow at the KU Leuven Centre for IT & IP Law. He is also managing partner of White Bison, where he advises data and AI-focused startups and scale-ups on commercial, corporate and compliance matters. Jan has previously worked at the Wilfried Martens Centre for European Studies and in the European People's Party Secretariat in the European Parliament. He holds master's degrees from the University of Warsaw and China University of Political Science and Law.

Credits

The Wilfried Martens Centre for European Studies is the political foundation and think tank of the European People's Party (EPP), dedicated to the promotion of Christian Democrat, conservative and like-minded political values.

Wilfried Martens Centre for European Studies
Rue du Commerce 20
Brussels, BE 1000

For more information, please visit www.martenscentre.eu.

External editing: Communicative English bv
Internal editor: Dimitar Lilkov, Senior Research Officer, Martens Centre
Typesetting: Victoria Agency

Printed in Belgium by INNI Group

This publication receives funding from the European Parliament.