The role of collective action in ensuring data justice

Five preconditions to protecting people from data-driven collective harms

Ausloos, J.; Toh, J.; Giannopoulou, A.

Publication date
2022

Document Version
Final published version

The role of collective action in ensuring data justice

Five preconditions to protecting people from data-driven collective harms

Jef Ausloos , Jill Toh , Alexandra Giannopoulou

1 December 2022

Reading time: 13 minutes

This is the final instalment of a three-part blog series that explores the potential of collective action, within and beyond existing legal mechanisms, as a means of redress against the harms of data-driven technologies.

Introduction

As we have seen in the first two blog posts in this series, the law hardly acknowledges the collective dimension of data-driven harms and the systemic asymmetries they contribute to and feed off . Unsurprisingly then, the law appears to be able to tackle these asymmetries only to a limited extent (as discussed here). The dire picture of insurmountable power imbalances, perpetuated and exacerbated by data-driven technologies, underscores the need to both emphasise the collective dimension of harms in our approaches to legal protection and law-making, and reflect on the role of the law in the fast-moving technology regulation sphere.

This task appears to be particularly urgent as a number of AI and data regulations are currently coming into force (the Digital Services Act, Digital Markets Act, Data Governance Act) and being refined (the AI Act, AI Liability Act and Data Act).

In the last instalment of this series, we thought constructively about how to move forward and identify five key preconditions to create a different culture of data protection and ensure that legal measures can effectively help safeguard both individuals and communities:

1. Overcoming compliance culture.
2. Ensuring transparency red lines through proactive regulatory intervention.
3. Avoiding regulatory inflation.

4. Empowering affected communities by meaningfully engaging with them.
5. Guaranteeing access to justice.

We focus on the need to consider the regulation of data-driven systems in the context of broader political and societal contexts. In particular, we consider the GDPR as one potential tool within a set of legal and non-legal strategies to resist, subvert and combat power hierarchies. We use this as a starting point to reflect on some shortcomings of (EU) law-making, and the broader role of the law in protecting the marginalised in data-driven societies.

Beyond compliance culture

While compliance with the GDPR (as well as any other area of the law) is an important goal, the way it is interpreted and operationalised is often constrained. Compliance efforts suffer from a narrow-focused framing that cannot encompass the multifarious issues likely to emerge when complex data-driven technologies and infrastructures are in use.

For example, when Greek and European authorities were questioned about the legality of fitting new refugee camps with the expansive monitoring and surveillance system Centaur (described in our first blog post), the official response from the relevant authorities emphasised the GDPR compliance of the system. It is important to note that following official requests from Greek civil society organisations, including Homo Digitalis, the Greek Data Protection Authority (DPA) has launched an official investigation into Centaur with respect to the Ministry of Migration and Asylum.

Similarly, in the case of the use of e-proctoring system Proctorio at the University of Amsterdam, the Amsterdam District Court confirmed the University's GDPR compliance. The reason given was that installing surveillance software on students' computers was the only way to ensure the necessary exam invigilation. This indicates a narrow-minded legalistic interpretation of the law, that fails to consider the ample evidence questioning the 'necessity' of this type of exam invigilation processes in the first place, especially in a post-pandemic context.

GDPR compliance cannot boil down to a mere box-ticking exercise, with little consideration for the broader context in which data collection and processing occur. A meaningful evaluation and recognition of potential impacts on individuals and communities is

necessary to shift from simple compliance-based narratives to a fairer data ecosystem.

The relevant responsible actors should start their analysis by critically questioning the reasons for adopting a data-driven technology in the first place. Using the example of Centaur, authorities should be able to first demonstrate in general terms the need for a surveillance system, before assessing the strict necessity of the inherent data collection and processing that Centaur requires.

Establishing the necessity of a system is a complex exercise that cannot be bypassed, and the mechanisms currently in place are evidently insufficient. Data controllers effectively claim the legitimacy of a chosen system (Article 35, Chapter IV) in data protection impact assessments (the main mandated safeguarding procedure in use), often by stretching the meaning of GDPR criteria or by benefitting from the lack of strict compliance processes for principles, such as data minimisation and data protection by design and by default.

This procedural practice can lead to a narrow norm-setting environment, because even if operating under rather flexible concepts (such as the respect of data protection principles as set out in a broad manner by the GDPR), their interpretation remains constricted and neglects to consider new types of harms and wider impacts.

Finally, both data protection authorities and those controlling data-driven technologies need to recognise that they can be held accountable for, and have to address, the complex harms and impacts on individuals and communities.

From a legal perspective, and as recognised under the GDPR's data protection by design and by default requirement (Article 25, Chapter IV), this means that compliance ought not to be seen as a one-off effort to be made when a data-driven system is first adopted, but rather as a continuous exercise considering the broader implications of data infrastructures on everyone involved. Perhaps more importantly, and because not all harms and impacts can be anticipated, robust mechanisms should be in place to enable affected individuals and communities to challenge (specific parts of) data-driven technologies.

While the GDPR may offer some tools for empowering those affected (e.g. data rights), they cannot be seen as goals in themselves, but need to be interpreted and accommodated in light of the context in which, and interests for which, they are invoked.

Relevant civil society organisations could play an important facilitator role in linking

collective harms that data-driven systems are likely to inflict on specific communities with sector-specific or community-specific interpretations of these harms.[1]

From nominal transparency to accountability

In the absence of meaningful transparency, it is particularly hard to expose and identify the collective harms generated and/or exacerbated by an organisation and its technological infrastructure, notably systemic injustices such as discrimination.

When it comes to platform companies, the systemic lack of transparency has been denounced for obstructing accountability mechanisms and independent research. Collaborative approaches to transparency, that is when transparency auditors work in collaboration with companies, may be productive, but can create undesirable dependencies and solidify power dynamics both in civil society and between the academic and private sector. Alternatively, adversarial approaches through scraping, repurposing APIs and using data download functionalities offer more independent methods but raise significant legal, technical and economic questions.

For these reasons, it is vital that legislators step in to establish robust and straightforward transparency mechanisms that enable a more holistic perspective on data-driven technologies and those who operate them. Such interventions need to be complemented with proactive efforts to empower enforcement agencies, civil society, academia and journalists to engage with the information obtained.

The current swathe of EU digital policy initiatives, some of which already promulgated as Regulations, come a long way in laying down a legal framework with meaningful transparency requirements. Yet, it is less clear how these requirements will be operationalised and lead to the expected accountability.

Looking ahead, we urge policymakers to put considerably more effort into cultivating the necessary engagement with transparency requirements, developing detailed guidelines, actively including marginalised groups, investing in robust enforcement mechanisms and more.

Changing narratives and avoiding regulatory inflation

The GDPR is not the sole, and arguably not always the most appropriate, legal framework to challenge the collective harms stemming from data-driven power. Data protection law

can be considered a baseline horizontal framework that needs to interface with other subject/sector/context-specific laws to meaningfully help minimise (collective) harm.

The last few years have seen a plethora of legal and policy proposals for tackling a variety of issues raised by technology and corporate power. While we do not wish to discourage legal initiatives reining in informational capitalism, we identify a number of important concerns.

First of all, at the EU level, the legal basis of virtually all these frameworks is Article 114 of the Treaty on Functioning of the European Union (TFEU), which means that (one of) their main objective(s) is to ensure the proper functioning of the internal EU market.[2]

This prioritisation can be in tension and contradiction with other values that the EU purports to uphold. Legislators and civil society should consider the broader ambit of rights, freedoms and interests at stake, in order to capture the appropriate social rights and collective values ordinarily left out of the internal market logic. This ought to be done by actively engaging with the communities affected by data-related harms and interfacing more thoroughly with pre-existing legal frameworks and value systems.

Secondly, as argued in the previous two posts of this series, the dominant narrative in EU techno-policymaking frames all fundamental rights and freedoms from the perspective of protecting ‘the individual’ against ‘big tech’. We argue that this should be complemented with a wider concern for the substantial collective and societal harm generated and exacerbated by the development and use of data-driven technologies by private and public actors.

Finally, the explosion of new/proposed laws can lead to regulatory inflation. We believe that more (law) is not always better. From the perspective of civil society and academia, the current EU legal output may well be described as a denial-of-service attack, where the few resources available to defend underrepresented interests are completely hijacked.

As the many proposals on the table are gradually becoming law (the DGA, DSA, AI Act, AI Liability Act, etc.), the sheer volume of rules is likely to overwhelm those they purport to protect and those they are meant to be enforced by, to the benefit of those with the power and resources to manage the operationalisation of the law.

For this reason, we argue that there should be more effective rules on lobbying, related to

transparency, funding requirements and funding sources for think tanks and other organisations. As already explained in the second post of this series, the revolving door between European institutions and technology companies continues to remain highly problematic and providing independent oversight with investigative powers is crucial.

Cultivating collective engagement

Calls for inclusion, particularly of people suffering collective and systemic harms, are not new in policymaking debates but have taken on a new-found dynamism in the context of digital rights.

Effectively and accurately addressing harms caused by data-driven technologies requires the inclusion of marginalised individuals and communities – who represent those directly impacted and harmed – in policymaking and advocacy across local, national and EU-level. The #BrusselsSoWhite hashtag has clearly shown the absence and lack of marginalised people in discussions around technology policymaking, despite the EU expressing its commitment to anti-racism and inclusion.

Meaningful inclusion requires moving beyond the rhetoric, performativity and tokenisation of marginalised people. It requires looking inward to assess if the existing work environment, internal practices, hiring and retention requirements are barriers to entry and exclusionary-by-design. Mere representation is insufficient without a shift towards recognising the value of different types of expertise, and seeing the experience and knowledge of marginalised people as legitimate and of equal importance to those of legal and policy experts.

Safeguarding affected groups from collective harms is a continuous effort that needs to be considered at every step of law-making, policy, agenda and strategy setting, litigation, advocacy and so on. Meaningful engagement with affected communities should not only be part of the creation and operationalisation of the law, but should continue throughout standardisation processes and broader discussions of technology and digital rights, including the co-determination of technologies.

Meaningful access to justice

In addition to meaningful representation and inclusion, those harmed (whether individual or collectives) should not have the primary burden of obtaining protection, especially

considering the warped information and power dynamics they already face.

One way forward is to install clear red lines on the prohibition of certain data-driven technologies and practices, as well as explicitly reversing the burden of proof on certain data rights. This would mean that individuals or communities can bring claims against the operators of harmful data-driven technologies, without being incapacitated by the lack of access to the necessary information to 'prove' that a collective harm has occurred.

While the option of litigation should remain open and accessible not only in theory but also in practice, it is important to insist that litigation cannot be the only way forward, particularly as harms are inflicted at a large scale.

As seen also in the previous posts, litigation remains a costly, unpredictable, risky and protracted way to ensure that rights apply. In the example of platform work, the ability of platform companies to make constant tweaks to their algorithms and unilaterally adjust their contractual terms makes it clear that reliance on litigation to obtain protection cannot be the main or only solution.

Ex-post redress mechanisms that are more easily accessible to those affected must be available and, while data rights manage to show some promise, they constitute by no means a silver bullet.

Conclusion

In this blog series , we have demonstrated how data-driven technological systems can produce and exacerbate power asymmetries, creating risks and harms at a speed and scale previously unattainable. While much attention is generally given to *individual* risks and harms, we set out to spotlight *collective* harms and explored the insufficiencies of the current regulatory landscape to counter them.

With this third and final instalment, we have drawn attention to the need to consider the larger political and societal contexts, when thinking about the regulation of data-driven systems. In anticipation of the many recently adopted and upcoming data and AI regulatory proposals, we suggest considering the GDPR (its inception, interpretation and enforcement) as a cautionary tale to reflect on the broader role of the law in protecting the marginalised in our data-driven societies.

This blog series is published in the context of our Rethinking Data research project, which

sets an ambitious vision for data use and regulation that can deliver a positive shift in the digital ecosystem towards people and society. Read our report here.

Project

Rethinking data and rebalancing digital power

Keywords

AI and data ethics

Data governance

Data regulation

Europe

Authors

Jef Ausloos

Jill Toh

Alexandra Giannopoulou

Related content

Blog

The case for collective action against the harms of data-driven technologies

Jef Ausloos , Jill Toh , Alexandra Giannopoulou

To what extent are the GDPR's data rights an effective tool for enabling collective action?

23 November 2022

AI and data ethics Data governance

Blog

How the GDPR can exacerbate power asymmetries and collective data harms

Jef Ausloos , Jill Toh , Alexandra Giannopoulou

Exploring how power asymmetries operate across the law and collective harms

29 November 2022

AI and data ethics Data governance ...

Report

Rethinking data and rebalancing digital power

Valentina Pavel

What is a more ambitious vision for data use and regulation that can deliver a positive shift in the digital ecosystem towards people and society?

17 November 2022

Data regulation Digital inequality ...