# 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?*

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

**Publication date**
2022

**Document Version**
Final published version

# How the GDPR can exacerbate power asymmetries and collective data harms

Exploring how power asymmetries operate across the law and collective harms

Jef Ausloos , Jill Toh , Alexandra Giannopoulou

29 November 2022

Reading time: 17 minutes

*This is the second of three blogs in a 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 seen in our previous blog post, the law hardly recognises collective action as a means to counter data-driven harms towards groups of people. Yet, data rights, as defined in the GDPR, could help challenge harmful effects and support collective action, at least in theory.

The GDPR does not operate in a vacuum. So we need to consider the broader political economy in which it sits, if we are to understand its limitations as well as how it could effectively help groups of people defend their collective interests.

The task is especially urgent as the GDPR is only the first of a series of data-related regulations recently approved at EU level, including the Digital Services Act, Data Governance Act and Digital Markets Act. As these enter into force and others are discussed (the AI Act, AI Liability Act and Data Act), it is necessary to consider how the EU flagship legislation on data protection, purported to regulate the foundations of the digital economy, has conceptualised power imbalances, as well as how its application has dealt with those imbalances.

Faced with the regulation of their core operations, powerful actors have been known to deploy a variety of tactics to push their own interests, while marginalising those of various

groups and ensuring that they will be un(der)represented throughout the lifecycle of the legislative instrument.

More specifically, large technology corporations with the resources to lobby legislators have an active interest in constraining legal provisions to the atomised, individual level, ignoring broader systemic issues and neglecting to address the negative effects inflicted on specific groups and collectives. Private actors yielding their power in law-making doesn't mean that the representative organisms of the European Union do not share their interests. Rather, this only reflects the profound imbalance of power and lack of representation of stakeholder interests at EU level.

In this second instalment of our series on collective action and the law, we consider how those controlling data-driven technologies apply their strength against both individual and collective interests throughout the different phases of the law, by charting its inception, how it is interpreted and applied, and, finally, enforced.

We find that the GDPR does not properly acknowledge the power asymmetries on which it is supposed to intervene – and is itself a product of them. As a result, the defence of collective interests appears only in passing in the text of the regulation and is scarcely used – if at all. The exercise of GDPR data rights as a tool to counter data-driven power asymmetries remains underdeveloped in general, with individual litigation becoming the most common means to enforce the law.

We argue here that this necessary recourse to litigation furthers power imbalances at the expense of affected and often-marginalised groups, who have difficulty collectivising and/or defending their interests, because they lack the know-how, recourse and time to claim their rights in court.

## Inception

Private-sector success in influencing legislative and policymaking processes is not new. While previously fervently opposed to regulation, technology companies have changed tactics to (re)shape and (re)frame it, according to their interests. In today's EU policymaking and legal landscape, technology companies have been adopting similar corporate lobbying strategies to tobacco and oil industries, seeking to translate their economic power into political power through a variety of means. Central to the strategies of

many of these big tech companies are the practices of regulatory arbitrage and regulatory entrepreneurship, either to avoid regulation, or to actively change the law.

With countless policy proposals set to regulate the technology sector, data and AI companies now spend around €120 million annually on lobbying EU institutions. As it stands, they are the biggest lobby sector – ahead of finance, pharma, fossil fuels and chemicals – in the EU by spend, and this is without counting 'softer' forms of influence, such as astroturfing and funding of a wide network of third parties – from PR firms, to consultancies, think tanks, SMEs, start-up associations and academic institutions – and fostering academia-to-industry relations.

These lobbying budgets allow private companies to have privileged access to EU decision-making, not only on an individual level, but also through collectively organised trade and business associations, which constitute a significant part of the lobbying universe. Indeed, the recent Uber Files brought to light a swathe of problematic lobbying efforts, including attempts at weakening the proposed EU Directive on Platform Work.

The GDPR and ePrivacy Regulation can be seen as the first clear examples of American technology companies' massive lobbying efforts. LobbyPlag.eu, a project that tracked the data protection legislation amendments, illustrated how directly into the GDPR.[1] Private tech companies dominated much of the legislative process, capitalising on inadequate transparency and ethics rules on lobbying, strategically obfuscating their work through a labyrinth of industry groups and consultancies, and exploiting the limitation of resources (time and internal expertise on specific policy areas) of other interest groups, and revolving door practices.

As mentioned already, powerful private actors have an interest in ignoring systemic issues, which underpin collective harms and that collective action could help counter, and in ensuring that the law focuses on rights articulated at the individual level. We have seen a recent instantiation of this logic, in the discussion on the role of 'data intermediaries'. Although intermediaries have been framed as a practical way through which the collective dimension of data rights could be given shape, their present currency is based on their economic potential.

Political actors have taken notice of this, including the European Commission, which has

recently passed its regulation on European Data Governance (the 'DGA'). Not incidentally, the DGA focuses mostly on economic objectives, is concerned with people's rights and interests only within the extent that it refers to empowering *individual* data subjects and frames intermediaries in terms of their supposedly 'facilitating role in the emergence of new data-driven ecosystems'.

These aspects of the law raise significant issues. Without clear constraints on the type of actors that can perform the role of intermediaries and their objectives, their legally entrenched model can easily be usurped by the interests of those wielding economic power, at the cost of both individual and collective rights, freedoms and interests. In our view, data intermediaries' positive potential in mitigating power asymmetries depends on their clear decoupling from the primacy of *individual* rights and their alleged economic potential.

## Interpretation and application

GDPR aims at ensuring a *fair* data processing ecosystem, considerate of all interests, rights and freedoms, as they are affected by personal data processing operations. It regulates an 'accepted exercise of power', creating a legal infrastructure that is supposed to introduce fairness into informational power asymmetries. This includes the creation of an 'architecture of empowerment', which is meant to enable individual data subjects, but also civil society and data protection authorities, to actively control how/if personal data is processed.

While the GDPR's Chapter III on 'the rights of the data subject' is its most evident manifestation, this architecture of empowerment fundamentally relies on a range of obligations that fall on the shoulders of data controllers – those individuals or private or public institutions that determine the means and purposes of data processing. These obligations – ranging from data protection principles (Chapter II) to controller's responsibilities (see Article 24 in Chapter IV), requirements of data protection by design and by default (Article 25) and data protection impact assessments (Article 35) – effectively constitute the backbone for data empowerment in the GDPR.

In the first instalment of this series, we highlighted the abstract nature and polyvalence of GDPR data rights and the flexibility of the legal framework overall. While this flexibility can

make the regulation useful for groups of individuals and communities in a wide array of often-unanticipated situations, it can also be easily co-opted or moulded by those in power. This is evidently the case, with big tech industry setting the tone on how the law is interpreted and applied in practice, unsurprisingly much to their own benefit and satisfying perhaps only the minimum requirements and standards. Examples of this behaviour range from problematic cookie-walls, to ignoring data subject rights, to vague and misleading privacy policies and much more. Combined with the general paralysis of enforcement agencies and the limited resources of civil society, this effectively places on individuals, collectivised or not, the burden to go to court, as the GDPR's architecture of empowerment fails to do its job.

If the GDPR is to achieve its stated aim of protecting 'fundamental rights and freedoms of natural persons' affected by the processing of personal data (as well as similar regulatory goals in future data or AI-related acts), more needs to be done to counter pre-existing power and information asymmetries. Legal norms alone do not suffice to resolve systemic (data-driven) injustices. This needs to be recognised and actively considered in the efforts by legislators and enforcement agencies.

The mere existence of a relevant legal framework is blatantly insufficient to effectively prevent collective harm. Public institutions bear a significant responsibility to translate abstract norms into concrete (sector- and technology-specific) legal tools, and to proactively ensure full compliance in high-impact areas, such as work, migration and education, taking into consideration the existing, also non-data related, power dynamics at play.

The role of civil society, both in making abstract legal norms concrete and collectivising around, for example, data subject rights, should also be acknowledged and cultivated. This becomes increasingly necessary against the backdrop of the proliferation of regulatory proposals.[2] Indeed, the GDPR can only play a role in resolving some of the collective harms we have exemplified in the first instalment of this series, if their collective dimension is more actively recognised.

## Enforcement

Enforcement is a necessary precondition in rendering both a legislative process successful

and a piece of legislation impactful. However, GDPR enforcement issues are already well-documented and partially due precisely to its heavy reliance on court litigation as a final – yet dominant and often only – means of resisting (collective and individual) harm.
Recourse to the relevant data protection authorities (DPA) is obviously another route to out-of-court resolutions, but their deliberation process is generally long, less efficient and unsatisfying to claimants. DPAs have been proven to be under-resourced and neglect 'little tech' – smaller tech firms of all kinds that, regardless of their size, contribute to layering the infrastructure of the digital economy.[3]
Even when they reach litigation, legal challenges are rarely seen under the light of power asymmetries that disproportionately affect the people bringing their claims forward.

**Challenging algorithmic management by Uber & Ola**

In the case of the Dutch ride-hailing drivers who brought Uber and Ola to court, to exercise their data rights with regards to profiling, automated decision-making,[4] transparency and fairness[5] of the platforms' algorithmic management systems – the Amsterdam District Court's adjudication evidently struggled to consider the technological developments and disproportionate power dynamics at play in the case as well as the actual needs of the drivers and their individual and community interests. Moreover, part of the reason these drivers exercised their data rights was to complement their efforts in a six-year long legal battle at the UK Supreme Court on employment status.

The Dutch court rulings illustrate that the wide scope of the GDPR results in courts being the main arbiter interpreting its provisions, situated within the broader development of 'techno-law', and the risks that come with that.

In these two cases, the burden of proving how they had been subjected to automated decision-making was placed on to the drivers/workers, rather than the private companies.

As in similar instances, the companies first made it difficult for drivers/workers to access their data by implementing convoluted and confusing subject access request processes.

Then, they dumped data files on the claimants in a variety of formats, that prevented subjects understanding their content. Placing the burden of proof on drivers/workers neglected considering the context of existing power asymmetries, and privileged the companies.

Additionally, the legal reasoning provided by the Amsterdam District Court for parts of the judgement in the Uber case used a narrow and sometimes contradictory interpretation of personal data, with terms and conditions, unilaterally set by private companies, being translated into universal legal norms. Again, the Court's reasoning seemed disconnected from the interests of the drivers/workers who brought forward the cases.[6]

**Challenging online proctoring by the University of Amsterdam**

Another instructive example of data protection litigation in the Netherlands involves Amsterdam University students, who contested the legitimacy of Proctorio, the e-proctoring software used to invigilate their exams. The court case, in this instance, faced different kinds of challenges in trying to frame its objectives using the GDPR.

Lacking clear alternative means of resistance and of claiming participation in the University's decision-making processes, the students contested the horizontal application of an evidently highly intrusive and discriminatory software, a decision made without even consulting the Student Council.

In this case, Amsterdam District Court looked at whether the proctoring software was compliant with the GDPR in a narrow sense and eventually ruled in favour of the University's decision.[7] The use of Proctorio was deemed necessary, i.e. no alternative solution could have been implemented to ensure the carrying out of the exams. Interestingly, soon after, the Italian DPA issued a decision to fine the University of Bocconi for violating the GDPR for the use of a similar proctoring software.

Both decisions relied on data protection law, but neither took into consideration the

collective discrimination that students suffered or the lack of consultation of the student representatives in the decision-making process that led to the application of the software.

These omissions by the Courts can be explained through a variety of factors, such as overall procedural constraints and insufficient pre-litigation strategy-building that could have appropriately emphasised the students' interests in the litigation processes.

These conflicting decisions – on similar facts and both ruled on the basis of the GDPR – demonstrate that the reliance on *ex-post* enforcement, especially through litigation, raises significant barriers, precluding certain groups of individuals from being efficiently represented and making adequate and impactful cases.

More generally speaking, the intricate litigation strategies of resourceful actors operating data-driven technologies raise barriers for claimants at every step. It is not uncommon to witness active efforts to prolong the overall litigation process, exhausting all available legal remedies, engaging in damage limitation and diversion tactics, such as frequently modifying the technological operations at stake, and concentrating court cases on procedural issues.

The lack of rigorous and strong public enforcement – both *ex ante* and *ex post* – combined with a general trend of over-responsibilising individuals allows industry actors to largely disregard court rulings or interpret and apply them in very restrictive ways. Furthermore, the growing number of EU technology regulation proposals, conflicting enforcement mechanisms, and limited resources to ensure robust enforcement will add to existing challenges.

In short, the high bar for litigation, in terms of resource requirements, expertise needed and time dedication, constitutes a significant barrier for often-vulnerable individuals and communities suffering harm. And even where courts (partly) condemn certain data practices, compliance with the respective judgements is often inadequate.

In conclusion, the abstract nature of data rights poses issues surrounding power and access regarding the interpretation of their provisions, when these rights are invoked in the context of collective action in court. This underscores the necessity for individuals to

organise and collectivise across sectors to build community, resistance and solidarity. The 'F**k The Algorithm' chant raised in protest against the 2020 A-Level exams fiasco in the UK, and the protests against the use of proctoring technologies in Dutch universities, among other cases, have shown the importance of critical engagement and rallying around discriminatory and exclusionary algorithmic systems.

These initiatives can be further sustained through organising with traditional unions, but also with grassroots-led movements and organisations engaging in legal and non-legal strategies, and assessing more broadly how data rights can fit within these efforts. While data rights can offer a useful rhetorical device, they have so far been inadequate in supporting collective action *in practice*.

---

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

# The role of collective action in ensuring data justice

Jef Ausloos , Jill Toh , Alexandra Giannopoulou

Five preconditions to protecting people from data-driven collective harms

1 December 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 ...