Why the DSA could save us from the rise of authoritarian regimes

Alexandra Geese 2022-11-08T11:47:49

The rise of extremist right-wing governments, as observed recently in Italy, is closely linked to the business models of large digital platforms such as Facebook and YouTube. Their algorithms polarise debates and stir up emotions because that enables them to keep people on their screens for longer and show them advertising. Our time is their money. But what does that mean for democracy?

The profit-making polarisation of debates favours angry content eliciting hate and fear. In political terms, those emotions are usually targeted by right-wing extremist movements and parties who thrive on spreading anger and fear. As a consequence, messages shared on the internet by right-wing extremists go viral and then quickly enter the mainstream via conservative media or politicians. A recent example is German CDU leader Friedrich Merz calling Ukrainian refugees “social tourists”, picking up a typical right-wing extremist narrative depicting war refugees as greedy people going after German taxpayers’ money. People who consistently counter such speech are often attacked with coordinated hate posts. A case in point is the Austrian political scientist Natascha Strobl, who is regularly forced to leave Twitter to shield herself from threats and insults. Such pile-ons also silence people in the political centre.

The Swedish democracy researcher Staffan Lindberg from the V-Dem Institute sees a clear link between polarisation and the success of autocrats – something that three years ago was considered a bold theory and has now become reality. Nobel Peace Prize winners like Maria Ressa are calling for restrictions to be placed on tech companies’ destructive polarisation-power with a 10-point plan; the UN Secretary General Antonio Guterres tweeted: “Social media platforms based on a business model that monetizes anger & negativity are causing untold damage to societies. Hate speech & misinformation are proliferating. Our data is being bought & sold to influence behaviour. We need regulatory frameworks to change this.”

The European Union’s Digital Services Act (“DSA”) is this framework.

No more: “Too big to regulate”

The Act initiates a paradigm shift in the thinking about the regulation of digital technology in general, and of social networks, in particular. The following considerations are inspired by Shoshana Zuboff, emeritus Harvard professor and author of the ground-breaking book “The Age of Surveillance Capitalism”.

The first fundamental change is that the DSA breaks with the previous paradigm whereby tech companies shaped the world largely unhindered. Their global nature,

their financial might, and their ability to reach billions of people and thereby influence public opinion seemed to make regulatory attempts impossible or ineffectual. The Act now puts an end to that futility. Democracy is alive and has the clear intention to set its own rules that Big Tech companies also must abide by. This is an important point because the previously prevailing opinion in Brussels and Washington was that technological developments were unstoppable, and society had to adapt. The DSA differentiates between technology, business models, and content moderation rules, and questions whether surveillance capitalism really is unavoidable. “Too big to regulate” no longer holds up.

Holding platforms accountable for what they do – not for their users’ opinions

The second paradigm shift is the systemic approach. Prior to the DSA, liability and freedom of expression were considered to be the main areas of action for platform regulation. But regulation focusing primarily on platforms’ liability for user-generated content is far too restrictive and leads to a dilemma. Platforms are given a normative responsibility to decide on users’ freedom of expression, thus gaining even more power in a realm of information which, due to its own profit-oriented mechanisms, is the reason why such masses of problematic content are generated in the first place. Legislators and judicial authorities would therefore relinquish even more power to commercial stakeholders, precisely the opposite of what regulation seeks to do. At the same time, large platforms cleverly used the notion of freedom of expression as a main focus in the public debate, thus singing from the same song sheet as the defenders of freedom of expression and human rights, who are quite rightly concerned about restrictions to freedom of expression online.

Especially in countries where the rule of law is not a given and state actions are more feared than those of private enterprises, this fear is more than justified. However, by restricting the debate to the question of liability and freedom of expression, we turned a blind eye on what the platforms were actually doing. Freedom of expression is best guaranteed in an environment in which women and minorities are not systematically suppressed by hate speech and where extremist opinions are not disproportionately reinforced by untransparent algorithms. That is precisely what platforms promote and effect. It is true in democratic states, but even more so in autocracies, as demonstrated by the most recent research by Amnesty International into Facebook’s role in the genocide of the Rohingya in Myanmar. „Facebook’s algorithms were intensifying a storm of hatred against the Rohingya which contributed to real-world violence,” said Amnesty International Secretary General Agnès Callamard.

The DSA opens our eyes to the bigger picture in this respect. Whilst honouring the hosting liability exemption privilege of the E-Commerce Directive, it places the focus much more on the platforms’ conduct through the regime of due diligence obligations. Transparency provisions, clear notice-and-action processes, internal complaint mechanisms, and independent dispute settlement authorities ensure

clarity in the moderation of individual content and finally give rights to users whose content is arbitrarily blocked or deleted.

Who knows what – Tackling information asymmetry

However, looking into the deeper workings of these very large platforms is even more important. Thanks to the contributions of Facebook whistle-blower Frances Haugen, the Council and Parliament built upon the Commission's hesitant initial proposal. The DSA now addresses some systemic issues. Not with finished solutions but rather with a toolbox which offers insight and concrete intervention options to the European Commission, national supervisory authorities, independent researchers and, unfortunately to a lesser extent, NGOs and thereby the public.

The systemic approach leads on to the third paradigm shift of the DSA. It tackles and hopefully reduces the information asymmetry. So far, platforms knew everything about us due to the extensive collection and analysis of our most private data. We knew nothing. The little we could say with any kind of certainty came from whistle-blowers like Frances Haugen and others.

The DSA now offers methods to obtain knowledge about how platforms work. The very large platforms have to write risk assessments in which "systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services in the Union" are identified, analysed and assessed. It is therefore no longer just a question of abuse of the systems by "malicious actors" but rather the intended workings ("design") of the social networks themselves. The list of the explicitly stated risk areas is extensive. It applies to basic human rights in general and to human dignity and data protection, as well as to public opinion-forming, elections, violence against women, child protection, and public health. The factors which must be considered explicitly in the risk assessments not only include rather obvious aspects, such as recommendation systems, algorithms, content moderation systems and terms and conditions, but also advertising and data practices.

All very large platforms are independently audited at least once a year. Moreover, the Commission, Digital Services Coordinators in the Member States, and vetted independent researchers will be granted access to large platforms' data. Civil society organisations are at least allowed to use publicly available data freely. That finally enables quantitative analyses and ensures that data access can no longer be used as a means to reward friendly researchers and hinder critical minds from digging deeper. These rules also afford valuable insight into the platforms' conduct. If supervisory authorities, researchers, and NGOs can pose questions and answer them in an evidence-based manner, it will be possible to use that knowledge to design platforms to promote democracy and freedom of expression, rather than hinder them.

The new Regulation also contains a new restriction on how platforms can use our data, from which they derive so much knowledge about our society. The DSA prohibits sensitive data categories as per the GDPR from being incorporated into advertising profiles. Furthermore, data from people known to be minors can no

longer be used for advertising purposes. The cautious wording reflects a weary struggle with two opposing positions: keeping the status quo, i.e., using all personal data for which consent was granted via questionable cookie banners in extensive profiles, versus a complete reform of the online advertising model, towards purely contextual advertising without the use of personal data. Prohibiting the use of sensitive data is especially relevant, given the leaked Facebook documents which show that Facebook (now Meta) is not structurally able to distinguish certain data categories from others and thereby fulfil its related obligations not only under the GDPR but also the DSA/DMA.

It is precisely these extensive data profiles that make polarisation in social networks so dangerous. The algorithms prioritise content which triggers negative emotions such as fear and anger. Extensive user data profiles enable strong personalisation, meaning everyone sees exactly the information that personally aggravates them. Polarisation is strongly personalised and keeps people at their screens. Platforms thereby increase their profits, whilst democratic decision-making processes, which require facts and objective discussions, draw the short straw. The UN Secretary General warns: "Our data is being bought and sold to influence behaviour." Data protection should not only be about protecting an individual right but rather about protecting whole societies from manipulation.

That is where the DSA comes in. It doesn't just scratch the surface; it takes a critical look at the actual causes of these major threats to our democracy: hate, incitement, misinformation, and surveillance. Behind its abstract wording are dynamic instruments to put an end to the surveillance practices of Google and Meta, in particular, which use data hoovers for advertising purposes and polarisation, and to expose the algorithms which push hate messages and false information to the top of the list, and thus completely blur public debate. It lays the foundations for precise analyses which legislators and regulators need to enact evidence-based policies and precise provisions for an internet where everyone's voice is heard.

Enforcement and global impact

Will the DSA revolutionise the internet? One thing is clear: it all depends on whether it is properly enforced. The enforcement of the chapter dedicated to the very large platforms is currently the responsibility of the European Commission, which is establishing a corresponding competence centre. Part of the financing comes from the fees to be paid by the companies to be supervised. That is good because highly qualified experts can then be employed with that money. In the long term, however, the competence centre and the supervisory body should be further developed into an independent European authority to prevent political influence. That is even more urgent, given the current developments in Europe. With Italian and Sweden now joining Poland and Hungary, there are two further Member States with extreme right-wing governments in power who could send commissioners to Brussels in 2024, who might have greater interest in maintaining polarising algorithms and extensive data collection than protecting democracy. The supervisory authorities in the Member States also play an important role. The rule that researchers must be accredited in the "member state of establishment", i.e., in the very country in which the Big Tech

companies can exercise most influence, is disappointing. There is a good reason why the European Commission has the bulk of enforcement tasks regarding Big Tech.

Despite justified criticism, the DSA has the potential to become a global standard. There has been huge interest from around the world, especially from the USA, but also from countries such as Brazil, Pakistan, and Japan. As the first democratic continent to present a well thought out law, we have the opportunity to set the course and save the internet from being monopolised by surveillance companies. A powerful and consistent enforcement at EU level and in the Member States will be crucial for its success.
