Handshaking with God: the 2022 Strengthened Code of Practice on Disinformation and its Impact on Digital Sovereignty

2022-11-08 18:11:24 Ylenia Maria Citino

1. How does it feel to hold sovereign prerogatives in the digital world?

In 2008, Nobel-laureate economist Joseph Stiglitz wrote that «self-regulation is preposterous»[1]. He was conferring on the worst recession since the 1929 Great Depression, namely about the bank sector proving unable to police itself to assess systemic risks.

As long as serious threats are looming over the rule of law and democracy in Europe, the strengthening of the Code of Practice on Disinformation[2] was a more than necessary action. It confirmed – if this was not clear enough – that self-regulatory techniques, while beneficial in specific fields, can otherwise be flawed and show significant limits in others, such as risk assessment and management (early remarked by Levin in 1967[3]).

The failure to ensure an effective commitment to the 2018 Code, as unveiled by the 2021 Guidance for its Strengthening[4], led to a stricter institutional setting. From now on, online platforms will be policed to comply with the number of issues arising from their activity, since the only way to succeed seems to restore pieces of regulatory sovereignty previously delegated[5]. But can States exercise a superior power implying sovereign rights in this field?

The issue of the cession of sovereign powers is intertwined with the debated topic of digital sovereignty. Since the notion of sovereignty is constantly reshaping and influenced by countless historical developments, digital sovereignty also results in an unstable concept. It may be beside the point to recall Hinsley's definition of sovereignty as «a final and absolute political authority in the political community»[6]. If it's still true that «the supreme power of making laws for the political society must lie legally with the Ruler»[7], then we have a more blurred vision of who this ruler may be in the digital ecosystem.

2. Digital Sovereignty, or the Ignis Fatuus on the Marshy Grounds of Democracy

Now that the rise of big online platforms challenges almost every facet of the traditional authority of the nation-state, testing the resilience of liberal Constitutions, academics find it hard to choose the proper theoretical dimension for such new guises of sovereignty. Useful guidance is procured by modern theories of international law, public law, political science, and philosophy[8]. Still and all, the researcher is forced to assume an interdisciplinary posture that leaves behind any dogmatic border, thus evoking in some way the ubiquitous dimension of the Internet.

That said, the epistemic problem of sovereignty in the digital world, pulling on the ropes of a democratic construction built on marshy grounds, consists of a major contradiction[9]: on the one hand, the notion is debated and eviscerated under a state-centered approach. On the other hand, the same wording is used for the opposite belief, moving from the anarchic techno-utopian statement that "networks", "data" or "technology" should reign sovereign in a territory where, by design, old-fashioned Westphalian states should simply "keep off" (see Barlow's Declaration of the Independence of Cyberspace[10]).

State-associated digital sovereignty faces private entities' increasing power in the cyber world. Information services providers, as obvious as it may be, claim private jurisdiction and regulatory authority on the networks they created. In other words, while states affirm prerogative powers on national issues online, most of them are escaping physical territorial borders. The recipients of network services are forced to blindly accept a standardized contractual framework, regardless of their nationality: they form an acephalous and stateless civic space, a virtually secluded "algorithmic society"[11].

Disowning material boundaries and borders between jurisdictions, platforms – especially the larger ones – may refuse to fully comply with the laws of the country where the user is based. They have the muscle to choose the most favorable court. Consequently, state legislation, as a core quality of sovereignty[12], is challenged by private law contracts in an unprecedented way. In a globalized economy, this may not sound uncommon. Though large platforms' services, being the new linchpins of civic and political debate[13], now constitute a fundamental underpinning for freedom of expression that cannot be tarnished.

3. The Torchbearers of the Strengthened Code of Practice on Disinformation

In light of the foregoing arguments, if states are left only with the *ignis fatuus* of said digital sovereignty, it follows that large providers are the torchbearers of the Olympic fire. To this end, some evidence can be found in the text of the 2022 Strengthened Code of Practice on Disinformation[14] (henceforth, SCPD), built on the ashes of the 2018 Code. It should be remarked how it is born as a complementary action to the Digital Services Act[15]: its voluntary nature now resides under the umbrella of the DS Package. SCPD embodies a shift towards co-regulation, now a leading regulatory technique in the information environment as foretold by Dittrich[16].

The question may be raised as to whether this new instrument postulates an "invisible handshake" between the State and private actors[17]. In retrospect, it is crucial to assess the attitude of the EU institutions, during the new Code negotiation process. Either they behaved like the recruiters of relevant stakeholders, in order to entrust them with regulatory tasks previously belonging to the public authority or, more likely, they only meant to provide their good offices towards the stipulation of a "covenant" between entities claiming to have quasi-sovereign power in their borderless territories.

This duplicity of forces is only apparent in the SCPD. I contend that the new Code, far from being only an antitrust instrument of cooperation, bears some resemblance to an international treaty, therefore validating the trend that considers the option of large platforms as quasi-public actors[18]. If this hypothesis turns out to be a twist of imagination, let yourself at least be influenced by the following arguments.

4. A Provocative Kinship Between the 2022 Code and… an International Treaty

First, for the negotiations to succeed, signatories expressed their willing consent to be bound by the 44 commitments and associated measures of the Code. Far from being a private transaction, the Code has a public purpose: addressing disinformation as a major challenge in Europe and taking action that needs to be balanced with the protection of fundamental rights. Besides big platforms – starred as Gods of the cyber world – this new version of the code embraces other significant players (33 in total[19]), such as civil society, disinformation organizations, or fact-checkers, to name a few. Of course, tech giants are more incentivized to take part in negotiations and, eventually, sign. However, it should be stressed that this does not depend on some kind of coercion from the authority: drivers of such decisions can be the threat of future liability or stricter regulation, pressure from users or relevant advertisers as well as reputational motivations. If the idea of a voluntary commitment to an obligation, excluding any form of subjection, does not clarify the sovereign dilemma, more insight into the SCPD can help.

One of the suggestions provided by the Commission's 2021 Guidance to reinforce the Code[20] is to set "tailored commitments" to obtain larger participation across stakeholders. This would in practice create an array of granular obligations, varying upon the subject and resulting in a very fragmented discipline. While, on the one hand, custom-made governance of disinformation issues reflects the peculiarity of each platform and service provided, on the other hand, it reveals the lack of a unitary conception of the problem and, perhaps, a strategy of bilateral concessions aimed at obtaining so far as possible the lowest common denominator.

Second, the formulation of reservations to the Code is the most blatant point of contact with an international law setting, especially Article 19 of the 1969 Vienna Convention on the Law of the Treaties (VCLT)[21]. The Code's apparent integrity is even more segmented by the opportunity to opt out from selected obligations. Each stakeholder's subscription document contains a section where the company can indicate an additional comment regarding each commitment or measure. In particular, he can specify the reasons «for not subscribing (at the service level), including clarification regarding relevance and pertinence to a service».

By looking closely at practical examples, we can agree that they are no different from international treaties' reservations. Commitment no. 20 reads that «relevant Signatories commit to empowering users with tools to assess the provenance and edit history or authenticity or accuracy of digital content». TikTok refuses to subscribe to it and explains that it considers that «it would be imprudent to commit to this measure at a time when the underlying technology remains unproven […] TikTok will assess whether such an approach would be beneficial, taking into account existing measures in place»[22].

Should this not be enough, Commitment 22 sets out that «relevant Signatories commit to provide users with tools to help them make more informed decisions when they encounter online information that may be false or misleading […]». Once again, TikTok opts out, explaining that «the implementation of the other commitments under the Code […] provide a comprehensive approach to tackling disinformation, including facilitating users […] when they encounter online information that may be false or misleading. […] As such, TikTok does not consider that committing to this measure will materially add to the other measures being adopted under the Code». In other cases, the reservation is more direct: «TikTok does not consider this to be a practical or implementable proposal. In any event, this measure is unnecessary […]». A similar position is held by other companies, such as Twitter, stating that «pursuant to the EC's guidance, Twitter intends to take the opportunity to explore the feasibility of this Measure».

Third, many international treaties often establish a committee of experts to monitor the implementation of the provisions by signing parties. Similarly, the Code establishes a "permanent task force". This body, gathering the Signatories, EEAS representatives, members of the European Regulators Group for Audiovisual Media Services (ERGA) and of the European Digital Media Observatory (EDMO), other third parties as well as officials from the Commission, with chairing duties, has the task to update and improve the Code.

Rather than a policymaker, the Commission acts more like an external controller, requiring cooperation in specific cases (Measure 40.6) or receiving data and reports delivered by relevant signatories upon request «in special situations like elections or crisis» (Commitment 42). The Code, following its voluntary nature, leaves no room for sanctions or other efficient methods of enforcement. These digital quasi-sovereign entities will establish their internal compliance mechanism. Broadly speaking, the role of the Commission only becomes more evident when we consider that the overarching commitments of the Code embody one of the possible risk mitigation measures required under Article 35 DSA from Very Large Online Platforms. This connection means that a voluntary withdrawal of one party from the Code may be evaluated by the Commission as a failure to mitigate such risks[23].

4. Conclusion

All this requires concise but interim conclusions. The ping-pong of sovereign prerogatives is a delicate matter when related to disinformation. Whether digital sovereignty pertains exclusively to states or is, *de facto*, shared with big tech corporations, is moot, and such a question would require gauging more elements through a more detailed exam[24].

Here, I only laid out a few cards on the table, some charming suggestions alluding that if there ever was a shift in sovereignty, it was a voluntary concession from platforms to the EU and its member states, not the other way around. In the end, they seem to prefer the novelties arising from such a negotiated form of obedience rather than capitulate in front of a more sharp-edged traditional legal approach. Conversely, if states want to conquer the new digital territories, extend their oversight on fundamental rights, protect their public order and avoid increasing platform-based privatization[25] , they simply cannot rely on gradual sectorial adjustments or hustle to keep up with the fast pace of technological progress[26]. Rather, they should gather their "legal armies" at the supranational level, maintaining a prolific dialogue with big corporates and demising the use of force in favor of the establishment of global constitutionalized standards.

* Ylenia Maria Citino, Post-Doctoral Researcher in Public Law – Luiss Guido Carli University

[1] J.E. Stiglitz, *Capitalist Fools*, in *vanityfair.com*, 9 December 2008.

[2] European Commission, *2022 Strengthened Code of Practice on Disinformation*, in *digital-strategy.ec.europa.eu*, 16 June 2022.

[3] H.J. Levin, *The limits of self-regulation*, in Columbia Law Review, 67-4, 1967, 603-644.

[4] European Commission, *Guidance on Strengthening the Code of Practice on Disinformation*, in *digital-strategy.ec.europa.eu*, 26 May 2021.

[5] L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in Philosophy & Technology, 33, 2020, 369-378.

[6] F.H. Hinsley, *Sovereignty*, Cambridge, 2nd ed., 1986, 26.

[7] *Ibid*.

[8] S. Besson, *Sovereignty*, in *Max Planck Encyclopedias of International Law (MPIL)*, 2011, 1-33.

[9] S. Couture – S. Toupin, *What does the notion of "sovereignty" mean when referring to the digital?*, in *New Media & Society*, 21:10, 2019, 2305-2322.

[10] J.P. Barlow, *A Declaration of the Independence of Cyberspace*, in *eff.org*, 8 February 1996.

[11] H.W. Micklitz *et al.* (eds), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

[12] L. Belli – P.A. Francisco – N. Zingales, *Law of the Land or Law of the Platform? Beware of the Privatisation of Regulation and Police*, in L. Belli – N. Zingales (eds), *Platform Regulations. How Platforms are Regulated and How They Regulate Us*, Rio de Janeiro, 2017, 41 ff.

[13] J. Naughton, *Elon, Twitter is not the town square – it's just a private shop. The square belongs to us all*, in *theguardian.com*, 1 May 2022.

[14] European Commission, 2022 Strengthened Code of Practice on Disinformation, cit.

[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), in EU OJ L 277/1.

[16] P.J. Dittrich, *Tackling the spread of disinformation. Why a co-regulatory approach is the right Wy forward for the EU*, in *bertelsmann-stiftung.de*, 12 December 2019.

[17] M.D. Birnhack – N. Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, in *Virginia Journal of Law & Technology*, 8-1, 2003, 1-57.

[18] G. De Gregorio, *From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society*, in *European Journal of Legal Studies*, 11-2, 2019, 65-103.

[19] European Commission, *Signatories of the 2022 Strengthened Code of Practice on Disinformation*, in *https://digital-strategy.ec.europa.eu*, 16 June 2022.

[20] European Commission, Guidance on Strengthening the Code of Practice on Disinformation, cit.

[21] Vienna Convention on the Law of Treaties, in *legal.un.org*, 23 May 1969.

[22] EU Code of Practice on Disinformation 2022 – Subscription Document for TikTok, in *digital-strategy.ec.europa.eu*, 16 June 2022.

[23] R. Fahy – N. Appelman – N. Helberger, *The EU's regulatory push against disinformation*, in *verfassungsblog.de*, 5 August 2022.

[24] See F.M. De Abreu Duarte – F. Palmiotto (eds), *Sovereignty, Technology and Governance after COVID-19: Legal Challenges in a Post-Pandemic Europe*, Oxford, 2022.

[25] M. Monti, *The EU Code of Practice on Disinformation and the Risk of Privatisation of Censorship*, in S. Gusti – E. Piras, *Democracy and Fake News: Information, Manipulation and Post-Truth Politics*, Abingdon-New York, 2021, 214-225.

[26] N. Cox, *The Regulation of Cyberspace and the Loss of National Sovereignty*, in *Information & Communications Technology Law*, 11:3, 2002, 241-253.