4.

THE EU: A FORCE FOR (DIGITAL) GOOD?

— JOSÉ IGNACIO TORREBLANCA

This paper examines how the digitization of information and the emergence of social networks have resulted in the weakening of liberal democracies and, in parallel, the strengthening of authoritarian regimes. To counteract the ability of foreign actors to disseminate narratives that delegitimize democracy, it proposes that the European Union should lead a grand multilateral agreement that, in the manner of Bretton Woods, establishes the framework for a democratic governance of technology.

THE WEAPONISING OF INFORMATION AGAINST DEMOCRACIES

Freedom House has documented 17 straight years of democratic decline around the world.[1] The result is that consolidated democracies are devolving into the illiberal. "Born again authoritarians" countries like Turkey that once had democracies and have regressed are no longer the exception. And, as the cases of Hungary and Poland prove, the decline is happening even at the very heart of the European Union, which claims to be the most advanced space for democracy in the world.

This global democratic decay represents a major geopolitical challenge for the EU, which has an existential interest in sustaining the multilateral liberal international order. As the President of the European Commission, Ursula von der Leyen, has pointed out, multilateralism, synonymous with a law-based order, is in the EU's DNA: it underpins its security and prosperity. However, as the EU has experienced only too well over the past decade, without liberal states (at home) a global liberal order is not possible: illiberal states and authoritarian regimes conceive of the international order as a destabilizing element from which to isolate themselves or in which to participate exclusively according to a logic of power, or, even, an existential threat they thus must undermine.

Among the various elements negatively impacting on the quantity and quality of democracies, it is worth highlighting two interrelated phenomena that profoundly weaken democracy: one, the increased political polarization and second, the loss of faith in elections. As we have seen in the U.S. with the assault on Capitol Hill and in Brazil when the three branches of government were stormed, the combination of both elements makes for a very dangerous cocktail.[2] This involution is the consequence of the systematic destruction of communicative, media, and political representation spaces of our societies as a result of the disintermediation facilitated by the new information and communication technologies, i.e., social platforms and networks.

The decline of democracy goes hand in hand with the rise of digital authoritarianism. On the one hand, authoritarian regimes are increasingly effective in suppressing dissent, controlling social networks and exporting surveillance technologies to third countries.[3] These regimes have found in the horizontal and open nature of these networks and in their inadequate or

non-existent regulation in many countries, a vulnerability to exploit against democracies.

Data shows that between 2014 and 2020, 1.7 billion people in 33 countries voted in elections that were interfered in by foreign powers.[4]

Democracies also experienced large-scale COVID-19 disinformation aimed at destroying public confidence in authorities, experts, institutions, and the media.[5]

The war in Ukraine has provided a good example of how vulnerabilities in the information space do not only harm democracy at home but can turn into major geopolitical and security weaknesses. As we saw, in the months leading up to the February 24th, 2022, aggression, the Russian disinformation machine was able to globally counter US warnings about the intentions of the Russian military deployment quite effectively. Strategies of denial, ridicule, and delegitimization helped to shape public opinion and encouraged European governments into believing that the military intervention was a US propaganda operation to stigmatize Russia, when its real goal was to prevent both NATO and EU partners from fully committing to the defense of Ukrainian sovereignty.

It is true that Ukraine has subsequently been able to build a very powerful narrative of its will to resist, which in turn has allowed it to sustain its war effort and garner vital moral and material support for resistance to the Russian invasion. At the same time, however, European authorities have found that outside EU borders, in what many refer to as the "Global South", Russia has been very successful at undermining the legitimacy of the European and US response. Although the Russian military has suffered severe defeats on the ground, as EU High Representative for Foreign and Security Policy Josep Borrell has noted, when it comes to the battle of narratives, the EU has been losing.[6]

THE EU COUNTER DISINFORMATION EFFORTS

The European response to this challenge is insufficient in large part because is being waged in a field, that of information and communication on social networks, in which the European Union and member states are not fluent or competent. In his recent speech to EU ambassadors meeting in Brussels in December 2021, Mr. Borrell rightly lamented the reactivity, lack of presence and ineffectiveness of European diplomacy in the global conversation on Ukraine and encouraged them to join the battle of narratives.[7] However, as one diplomat in the room rightly criticized: 'we are being asked to respond to an industrial disinformation operation by tweeting a little more every day'. The EU's frustration is understandable, but to overcome it Brussels will need to understand how and why it has reached the situation it finds itself in.

The EU has taken some important steps in regulating social media already. In 2018, it published its first communication on disinformation.[8] It then invited large platforms to join a process of information sharing, transparency, and best practices through which it was able to get companies to start actively engaging in and be held accountable for taking down fake accounts, detecting coordinated inauthentic behavior (CIB), and monitoring the truthfulness and authenticity of political advertising. With the approval of both the Digital Services and Digital Market Acts (DSA and DMA), the EU has shown great determination and vision to contain the most damaging effects of social media platforms and networks on democracy. In this task, it has undoubtedly been helped by the pandemic, which has made clear that disinformation can have a powerful impact on public health and should be considered a social risk of the first magnitude. As a result, society, the media, public opinion, and governments have changed their perception of the risks associated with social networks and begun to act within their respective spheres of competence to counteract these trends.

Two criticisms of the EU that should be flagged are that this determination has been inward-looking and primarily defensive, rather than offensive or proactive. The result is that globally, starting with the U.S., the

lack of or inadequate regulation of social networks continues to threaten the integrity of democracies and their communicative and deliberative spaces.

The EU cannot be triumphalist. Its program of strategic autonomy or (more ambitiously) "digital sovereignty" is far from complete when it comes to preserving democracy from the misuses and abuses of technology. On the one hand, the regulatory success of such rules as the DSA remains to be demonstrated in practice: its deployment and implementation will be slow and fraught with difficulties, both on the part of governments (since member states bear a large part of the responsibility), and of social platforms and networks, whose commitment to this regulatory agenda, as the cases of Tik Tok and Elon Musk's takeover of Twitter show, are weak, fragile, or non-existent.

On the other hand, European initiatives to fight this global battle of narratives need a major update. The pioneering anti-disinformation service launched by the EU's External Action Service, East StratComm, built a catalogue of nearly 15,000 pieces of Russian-sourced disinformation. This repository has educated a whole generation of politicians, journalists, and experts on the complexities of disinformation narratives, but this massive effort is proving to have the same limitations as the fact-checking processes undertaken by civil society and the media. Disproving or classifying information as false is necessary, but this disproval does not automatically reach the people who consumed the disinformation; they are located in communicative bubble-spaces that are immune to these processes. Verification neither acts on the ecosystem in which disinformation is disseminated nor acts at source against those responsible for its creation and dissemination. It is, therefore, a partial and very incomplete tool.

Acting on the digital ecosystem requires well-honed legal capacities, and herein lies the importance of the DSA. Acting at source is especially complicated because whereas the EU adopts a defensive, legalistic, and protective position to establish attribution processes based on empirical evidence and the use of legal instruments (police, prosecutors, judges, and courts), the actors that develop influence strategies act offensively and with long-term strategy according to a logic of power and conflict that in many cases is analogous to that of warfare. As RT's director Margarita Simonyan revealed, Russia's networks of influence and interference are not spontaneous: over the last few years, Moscow has developed a long-term strategy to create and cultivate loyalty among audiences in the West who could be mobilized at critical moments to defend its positions, weaken the Western consensus, and delegitimize its messages and institutions.[8] Such a long-term media strategy that includes TV channels as well as digital and social media is something the EU lacks (and is hardly available to a government apparatus in a democratic society).

Thus, in its fight against the abuse of technology to undermine democracies, the EU is doubly hamstrung by a defensive and legalistic logic that prevents it from acting proactively and in accordance with a geopolitical and security logic. What can it do about this, and what is it doing?

A DIGITAL BRETTON WOODS

As a result of reflection on the EU's insufficient external activism in digital matters and concerns about both the growing intersection between geopolitics and technology and the rise of digital authoritarianism, the EU adopted its first external digital diplomacy in July 2022.[9] This strategy sets out the need for the technological and digital component as a central element of the EU's external action and aims to combine and coordinate under a single strategy element of political action that have hitherto been scattered, e.g., external action aspects of the cybersecurity strategy, the action plan on democracy or the fight against hybrid threats, including foreign information manipulation and interference (FIMI).

In addition to this coordination, the Council invited the Commission and the High Representative to work closely with like-minded countries, both bilaterally and regionally, and multilateral organizations to maintain an open, free, global, stable, and secure Internet based on a multi-stakeholder approach. In doing so, the EU consolidates its vocation to the global governance of technology with the aim of imprinting on this governance its humanist and rights-based vision of technology or, as the Council puts it, the shaping of "ethical, safe and inclusive international technology standards." Special attention should be paid to the expression of the will to act on "countries of strategic importance that have a high level of vulnerability," to combat Internet shutdowns, arbitrary or indiscriminate digital surveillance and data retention, to protect human rights defenders and civil society online, and to expand civic spaces.

This is an ambitious agenda that requires coordination between multiple levels both within the Commission and between European institutions and organizations. Just as important, if not more so, is that such a strategy requires close and in-depth dialogue with third actors, both bilaterally and multilaterally.

Some, e.g., the Trade and Technology Council (TTC) with the United States and digital partnerships with Japan, Canada, and Korea, are already underway. The EU has also shown its vocation to coordinate its strategies with Indo-Pacific countries, the African Union, and Latin America and renew its cooperation in the framework of such organizations as UNESCO, the ITU, and the OECD.

If the EU is to become this "force for digital good," it will have to go much further. As has been said many times, the weight, power, and attractiveness of its internal market turns the EU into a de facto regulatory superpower. The accumulation of legislation on digital and technological matters approved by the EU in recent years that covers everything from data to AI, digital markets and services, and cybersecurity undoubtedly makes the EU the most densely regulated digital and technological space in the world and a benchmark for many countries (not least of which the U.S.) to imitate.

Ideally, with all these regulations in place and with their successful implementation, the EU would be in a position to claim to have achieved its desired goal of strategic autonomy (or, at least in part, "digital sovereignty"). With respect to the rest of the world, it could rely on the "Brussels effect" popularized by the conversion of its European data regulation (GDPR) into the global data gold standard. But would that be enough? Or credible? As with security, the risks and threats posed by technology are not divisible in a global market and such a conflict-ridden geopolitical environment. As in so many other matters, even if it could, the EU cannot aspire to standards so high that by their very cost and nature they are unattainable by the rest of the world. A "Galapagos effect" that renders the EU so advanced in its rules that it cannot relate or deal with anyone is simply not possible nor desirable.[10] The EU must therefore think in terms of global governance. This requires seeking to empower third parties, be they governments, parliaments, independent institutions, civil society, or experts outside Europe.

One of the great difficulties in this task is the relationship with the U.S. In a world dominated by geopolitical rivalries and high-voltage tensions between the West on the one hand, and China and Russia on the other, there is not enough room for two models of digital governance as opposed to each other as the European and the US. In an ideal world, the U.S. and the EU should be able to design together with other like-minded OECD and Global South countries a digital governance architecture equivalent to the Bretton Woods system achieved after World War II. If back then an international liberal order was tailored to merge and satisfy both the material needs and the moral aspirations of liberal democracies, the challenge today would be to achieve a multilateral digital liberal order compatible with liberal values, or at least as broad a sphere of rights-based technological governance as possible given that China and Russia would refuse to be part of such an order.

The US polarization precludes Washington from becoming a driving pillar of such rules-based global governance. And even if legislation matching the EU was approved by the Democrats or through bipartisan agreements, uncertainty about the reversibility of any international agreements the U.S. might eventually commit itself to would be very high. Although many domestic actors in the U.S. (states, cities, civil society) aspire to this regulatory convergence with the EU that could eventually become a template that could be extended globally, the difficulty of bi-partisan consensus and the classic reluctance of the executive and legislative branches to reach internationally binding agreements make it very difficult to take this first step. For this reason, although agreement between the U.S. and the EU is not a sufficient condition for global governance, it is a necessary one.

There is a plethora of actors in the Global South and the G-20 orbit (India, Brazil, and others) whose cooperation and contribution are also essential. For both the U.S. and the EU, talking and agreeing with these actors is extremely difficult not because their alignment with democratic and liberal values is weak or fragile (where are they not nowadays?: as it is said, “let he who is blameless cast the first stone”) but because their vision of international order and global governance is mediated by their past negative experiences with the West. Many of these countries conceive of the multilateral order as a purely Western artifact aimed at safeguarding Western power and excluding others. Their participation in such an enterprise cannot be taken for granted.

CONCLUSIONS

Convergence among democracies must come from below and not from above. Actions speak louder than words such that when countries see the tangible benefits of such a model, they will make it their own out of pure self-interest. Just as after the Second World War, when the U.S. and the other liberal democracies managed to fit their economic and security interests into a multilateral framework that was also liberal, the challenge for the EU today is to offer liberal democracies a model of embedded multilateralism in terms of global internet governance.

As a matter of both interest and principle, the EU's DNA demands the same approach to the governance of technology as to health or the environment: as a global public good to the provision of which it contributes decisively, even if unilaterally at first to establish a tit-for-tat model of cooperation.

Just as God can write straight with crooked lines, the EU can unilaterally promote technological governance in the interest of all by going solo at the beginning and then invite others in to try and set up a multilateral framework regulating digital technologies for the benefit of all.

ENDNOTES

1 Freedom House. (2023). Freedom in the World 2023: Making 50 years in the struggle for democracy, https://freedomhouse.org/sites/default/files/2023-03/FIW_World_2023_DigtalPDF.pdf

2 European Council on Foreign Relations. (n.d.). Power Atlas: Culture, https://ecfr.eu/special/power-atlas/culture/#weaponising-the-vulnerabilities-of-other-systems-rather-than-being-a-city-on-a-hill

3 Freedom House. (2022). Freedom on the Net 2022: Countering the Authoritarian Overhaul of the Internet, https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet

4 Australian Strategic Policy Institute. (n.d.). Cyber-enabled foreign interference in elections and referendums, https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

5 Facebook. (2021). IO Threat Report May 20, 2021, https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf

6 European External Action Service. (n.d.). G20: Difficult times for multilateralism, https://www.eeas.europa.eu/eeas/g20-difficult-times-multilateralism_en

7 European External Action Service. (2022). EU Ambassadors Annual Conference 2022: Opening speech by High Representative Josep Borrell, https://www.eeas.europa.eu/eeas/eu-ambassadors-annual-conference-2022-opening-speech-high-representative-josep-borrell_en

8 EUvsDisinfo. (2018). Chief Editor: RT is Like "a Defence Ministry", https://euvsdisinfo.eu/chief-editor-rt-is-like-a-defence-ministry/

9 Council of the European Union. (2022). ST 11406 2022 INIT, *https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/en/pdf*

10 *Ibid.*