The Regionalization of the Internet

Angelos Kaskanis

The interface between the internet and physical reality becomes ever more dense, particularly during a pandemic. In parallel, there is a tendency of fragmentation in what we perceive as a global internet network, or "regionalisation." The vision of the libertarian and self-regulating internet space of the 1990s is giving way to censorship, the nationalisation of data, corporate oligopolies, and mass surveillance.

The libertarian notion of the internet is fighting back with digital currencies, virtual private networks, e-residence, and anti-systemic online activism. But the state is also struggling to re-assert some of its authority over currency, taxation and the public sphere while making the most out of new possibilities in surveillance and policing.

Central banks are moving into digital currency markets, there are increasing demands for editorial responsibility from social media platforms, countries are demanding the repatriation of data storage, and we have even seen the emergence of "data embassies." Many regimes are constructing panopticon digital architectures, exploiting historically unprecedented surveillance technology.

We ask how different regions of the internet balance public and private interests in this fragmented cyberspace. We invite in this conversation Spyridoula Markou, a professional fact-checker, member of IFCN and Facebook's third-party fact-checking partner based in Greece; Bojan Stojkovski, a freelance journalist who has been covering foreign policy and EU affairs for more than a decade and Atdhe Lila, a legal consultant, specializing in privacy, cyber and IP Law.

AK: How much ownership over their data do people have in different internet regions?

Spyridoula Markou: The right of citizens to access their data is not related to the state of economic development but to the political regime. In countries with authoritarian regimes such as China, Belarus, the United Arab Emirates, etc. the "fishing" of data - the processing and, ultimately, the use of the intelligence - is not yet known to the public.

Governments that prioritise maintaining the status quo over advancing the standards of living of their citizens naturally have different data management protocols.

However, differences in data ownership are also found between democratic European states. After the adoption of the GDPR regime in Europe, data management regulation was in part aligned so as to render individuals owners of their own data. But not everyone applies regulation faithfully, particularly in Balkan states or new EU member states.

Bojan Stojkovski: It seems to me that the regulatory framework for data ownership is somehow still incomplete, in the EU as elsewhere. It is not always clear how users have control over their digital data and, also, how significant are the potential violations of data ownership guidelines.

Regarding the EU, there are no comprehensive policy frameworks at the national or Common market level when it comes to data ownership. In general, internet regimes are not transparent and are difficult to compare.

Atdhe Lila: Digital data has become one of, if not the most valuable resource. This makes it very clear why so many companies and governments mine data and are not very eager to give citizens ownership of their own data.

After the adoption of GDPR regulation in the EU, data processing has become more limited and this has given citizens more control over their data. The same is happening now in other developed countries since the EU refuses to cooperate with countries that do not foster the same level of protection. However, more control does not constitute data ownership. There is still a lot to do for citizens to have actual ownership over their data. Some scholars have even proposed that citizens whose data is used should be financially compensated.

AK: What is the digital frontier between autocracy and democracy?

Bojan Stojkovski: I think that the digital frontier between autocracy and democracy can often be seen in effect rather than in principle. Authoritarian regimes use similar surveillance, repression, and propaganda technologies for mass control. They tend to strengthen their authoritarian rule through these tactics, coupling surveillance with censorship. In this sense, the digital frontier becomes visible when we focus on case studies of digital instruments used by authoritarian regimes to maintain their stronghold.

Spyridoula Markou: Freedom is the ability to avail of all available opportunities, provided one respects the freedoms and rights of their other digital fellow citizens. In practice, this freedom is limited both semantically and in practice.

The noticeable difference between regimes lies in the exploitation of citizens’ digital data, where exclusive ownership of their data does not exist. Instead, there is exclusive management by those who “mine” the data, third parties, mostly private organizations, for financial benefit. Therefore, in some cases, this limit is not based on an ideal, such as that of democracy, but is drawn in economic terms.

Atdhe Lila: Unlike physical reality, the line between autocracy and democracy online is rather difficult to identify. Technology can very easily be used to change peoples behaviour or to stop them from doing certain things, without them even noticing, especially if they do not belong to the minority with the technical skills to overcome officials barriers.

Even some of the more democratic countries have been found to be surveilling their citizens, their partner countries and corporates. The internet might have begun as one of the most democratic and open projects known to mankind but that is certainly no longer the case. It takes quite a lot of skill to avoid surveillance. Regulation should move towards data ownership, either on a state by state or regional level.

AK: And how do we share our internet region with non-democratic allies?

Atdhe Lila: The nature of the internet makes it almost impossible to ‘divide’ the internet between democratic and non-democratic allies. Perhaps in the future, we would be able to divide the internet into different ‘levels’ however this also poses numerous issues, as it would go against the very principle of internet neutrality, and we have seen that that has caused quite an uproar among citizens worldwide. What democratic countries might do is expel non-democratic countries from international organizations that manage and deal with internet-related policies, such as ICANN and maybe prohibit data sharing and internet related services to such countries.

Bojan Stojkovski: As a global phenomenon, we are inclined to share the internet with democratic and non-democratic allies alike, so the best we can do is bolster digital literacy and be aware of the potential dangers that lurk online, recognising threats and fending them off. The globalization process has also made the global cyberspace even more “local” I’d say, so the best way is to recognize and act against potential threats that are coming from non-democratic countries and regions. One must be wary of those threats and be ready to react at any time.

Spyridoula Markou: Reduced access to applications and data in authoritarian regimes is one of the problems faced by citizens. This, in turn, limits the sharing of information between peers. VPN use is often chosen by a small number of people with a high level of digital literacy, whose number is small in non-democratic countries.