

**OECD Webinar**  
**Reinforcing Democracy and Civil Space**

**"The impact of national and global security measures on civic space"**  
**15 July 2021**

*Remarks by Rafael Zanatta, Director of Data Privacy Brasil*

Thank you very much for inviting me to participate in this important webinar. The Civic Space Observatory's initiative is crucial at a time of threats to fundamental freedoms and rights.

This subject has been much discussed in the networks that we participate in, in particular the Coalition on Rights in the Network in Brazil and in the CSISAC (OECD's Civil Society Information Society Advisory Council on the Digital Economy Policy).

As a Latin American activist, the first point I would like to make is that the concept of terrorism, as mobilized in regional norms and practices, has a connection with our dictatorial past. In Latin America, terrorists were the subversive citizens. Citizens of the Left. The terrorists were not the enemies "from the outside", but the enemies "from within". This pattern still holds today and needs to be considered as new legislation on terrorism is formulated.

The pandemic brought a set of new problems such as the roll out of newer surveillance technologies and a relevant increase in data collection in order to allow for more covid control mechanisms. Apart from setting an enforcement date to our own Data Protection Law, one of the few victories we had was the affirmation of the protection of personal data as an autonomous fundamental right by the Federal Supreme Court. The Court decided that the pandemic cannot be a space of exception that legitimizes violations of fundamental rights. As we say in Brazil, data protection is part of the vaccine for Covid, in social terms.

This timid victory, however, is small compared to other threats. Over the course of the past years, we have witnessed the recent cases of indigenous leaders harassed by the Federal Police for their online demonstration against the federal government, the creation of digital dossiers on anti-fascist police officers by the Ministry of Justice and the acquisition and deployment of surveillance technologies such as softwares for monitoring political opponents, generally using technologies for aggregating "open data for intelligence". Another process worth mentioning is the increasing use of the National Security Act, a legislation from the Brazilian dictatorship period, as a tool to silence and shut down the opposition.

In the region, we see three very troubling trends in counterterrorism that impact civic space and our rights.

The first trend is the attempt to expand terrorism into cybersecurity issues. There is a concerning militarization of the field of personal data protection that might come along with more general misconceptions re. access to information and other topic Added to that, we are seeing attempts to conceptualize the attacks on critical infrastructure as terrorism issues, in legal terms. As reported by the Igarapé Institute, it is worrisome to relate cyber security with issues and competences of military institutions. In Brazil, the military has dominated much of the cybersecurity debate. This trend shifts the meaning of personal data protection, which is about people, freedoms and abusive discrimination - and not about sovereignty and national security.

The second trend is the attempt to include financial crimes and ransomware attacks as terrorist activities. Over the course of the years, there has been a considerable amount of pressure from traditional financial institutions (big banks) to redefine criminal law on financial scams and device hacking. This has led to an extremely worrisome scenario of increased criminalization of conducts and reforms to current laws that whilst trying to target the previously mentioned practices might have an impact on civil liberties as well. There are enormous risks for journalism and data activism, considering that system and device intrusions could be considered terrorist acts. We need to be very cautious about the expansion of the concept in the international arena.

The third trend is a narrative modeling on what constitutes conduct of "extreme violence" in the online environment. In Countries such as Colombia, content produced by civil entities and activists is sometimes considered to be "inciting violence". The government has pressured technology companies to enforce human rights standards and remove such content, because they violate rights. It is a subversion of logic.

Intermediaries cannot give in to these attempts, which can amplify the massive removal of legitimate discursive content by civil society. In a report on current approaches to violent and extremist content released after the Christchurch incident, the OECD highlights the importance of transparency in such policies and procedures.

Moreover, it is a concern among civil society entities that broad and undefined definitions of "terrorism" and "extreme violence" may represent illegitimate restrictions to human rights, such as the right to freedom of expression and the right to information in investigating issues of public interest. The lack of clear delimitations of what these terms mean for the purposes of legality and human rights protection online can stimulate this tactic of harassing and threatening by authoritarian governments.

For Latin American activists, this can be extremely dangerous. I thank the Civic Space Observatory for opening up this discussion and considering voices from the Global South.