Technological and digital sovereignty

Problem to be solved

Technological and cybernetic development has had a deep and accelerated advance, in a few years they have become an essential part of our lives. Computer programs or *software* and the devices through which we use them, or *hardware*, allow the control and management of a multitude of information and knowledge. From ordering a pizza to the most critical security operations of a State are mediated by these supports, and in their interaction billions of data are generated, valuable information that allows modeling social, political and economic behaviors.

Currently our development, research and technological innovation depend on large companies or corporations, mostly foreign, whose objectives respond to their own interests and business and market strategies, sometimes being distant and even contradictory to the strategic needs of our State and the aspirations of good living of its inhabitants. The use of monopolistic infrastructure and proprietary software generates a great loss of autonomy and independence in the administration, design, management, control and auditing of strategic resources for the functioning of the State and society.

The development, autonomy and protection of our territories, bodies, data and virtual interaction must be considered a structural and strategic part of our sovereignty.

Ideal situation

A sovereign state should consider the following strategic aspects:

- **Critical infrastructure**: Autonomy, control, audit and design over technologies, data and other sensitive aspects such as communications, national security, justice, public services, among others, is necessary.
- **Economy**: Taking care of the investment of public resources, strengthening circular economies and developing the productive matrix through a knowledge economy, local entrepreneurship and the development of innovation at all levels. Safeguarding the sustainability of its natural resources such as lithium, rare soil and others essentials for the creation of the entire technological infrastructure.
- **Science and knowledge**: Strengthening knowledge as a public good that cannot be privatized. Development of innovation as a strategic factor for progress. Ensuring both access and the possibility of generating new knowledge.
- **Education**: The integral formation of citizens who are creators of technologies and knowledge, providing the necessary tools and resources through public, free, egalitarian and quality education.
- **Data**: Our data should be considered a strategic asset, and should not be subject to public or private abuse. It is necessary to create an institutional

framework to protect sensitive data, as well as to educate about it.

What should be included in the new constitution

The new constitution must contemplate the *cyberspace* and the infrastructure that supports it as a sovereign and strategic space of the State, within a conception respectful of human rights and nature, in order to allow its autonomy while promoting its progress and development.

The constitution must guarantee and protect all the strategic aspects listed above.

With what arguments do you or your organization support this proposal?

The state must understand and be able to strategically establish the use of technologies that allow its sovereignty.

The world's leading economies have a strong investment in technology, which is reflected in their greater development and innovation, as well as in a high degree of specialization in the training of their professionals. Our country is the one that invests the least in research and development in the OECD, so a greater investment is necessary to progressively improve our productive matrix, providing us with greater technological autonomy.

Training in technologies that allow creativity, collaboration and solidarity is essential for progress in conditions of possibility for all inhabitants, as well as the freedom of our State to collaborate voluntarily with other entities.

It is also observable that the creation of users dependent on proprietary technologies has repercussions on the renunciation of personal autonomy and, in the long term, the renunciation of the sovereignty of public institutions.

Technological dependence on centralized and/or monopolistic infrastructures, programmed obsolescence, software licenses that expire, as well as programs that cannot be audited because they do not have access to the source code, and therefore potentially subject to the existence of "back doors" that enable espionage of national institutions and industry, are bad public policies that can cause serious damage to our economy and sovereignty.

Data, which includes information generated by all of us, is a valuable resource necessary for the creation of public policies that promote the development of the nation. It is relevant to generate all possible instances that prevent its depredation and malicious uses in order to protect the sovereignty of our peoples.

Emblematic cases of infringement of sovereignty in the technological field can be consulted in the attached bibliography.

Proposed articles

Primary duties of the State are:

1. To recognize cyberspace as a common dimension of interaction between humans and machines.
2. To recognize cyberspace as a strategic infrastructure built on hardware and software.
3. Defend national sovereignty in cyberspace.
4. Guarantee autonomy in the access, use and development of hardware and software technology, without prejudice to the possibility of voluntary collaboration with various communities, companies and states.
5. To protect personal and strategic data generated in the interaction with cyberspace.
6. To guarantee universal and comprehensive access to digital technology and cyberspace, incorporating information and communication technologies in the educational process.
7. Recognize and safeguard collective knowledge and wisdom from private appropriation, such as in the fields of science, culture, technology and ancestral knowledge.

Bibliography

- Porcentaje gasto PIB en investigación y desarrollo Chile
- "Afirma que los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos" Resolución Naciones Unidas: Promoción, protección y disfrute de los derechos humanos en Internet
- **Cambridge Analytica**: In the USA, the company carried out a large part of Donald Trump's campaign, with big data studies, generation of fake news, etc. It has also been similar in other countries, such as Argentina with Macri and in the UK for the Brexit; citizens' data have been used to manipulate public opinion.
  - Escándalo Facebook-Cambridge Analytica
  - Elección de Mauricio Macri que utiliza los servicios de Cambrdige Analytica
- **Spying on Merkel and Macron**: These were spying operations by the USA and Morocco on the presidents, software was infiltrated into their devices to monitor their communications.
  - EE.UU. espió a Angela Merkel entre 2002 y 2013, según reporte
  - Software israelí Pegasus espió a Emmanuel Macron y otros líderes
- **Snowden, Assange and NSA**: The NSA was exposed as an institution of technological espionage, discovering that the world's communications that pass through U.S. territory, that is, a large part of the Internet, are

monitored. Snowden took refuge in Russia and Assange in the Ecuadorian embassy of the United Kingdom, who is currently undergoing an extradition process. In this case, the privacy of individuals, freedom of expression and the sovereignty of nations are violated.
  - Edward Snowden, Wikipedia
  - Julian Assange, Wikipedia
- **Sosafe**: A citizen security application that already has contracts with municipalities such as Santiago, Ñuñoa, Providencia, Las Condes, La Pintana, among others, has become quite popular recently. According to the same media, Sebastián Piñera would have used Instagis software to develop his electoral strategy during the last presidential campaign that made him president.
  - Alguien te mira: así funciona el gigante de las campañas políticas que controla Sosafe
- **Intel ME**: Intel processors contain a subsystem called the Intel Management Engine (ME) that functions as a separate processor that cannot be disabled, potentially acting as a powerful undetectable remote backdoor.
  - Intel's Management Engine is a security hazard, and users need a way to disable it
- **Stuxnet**: During 2010, a system capable of reprogramming industrial facilities was discovered, which was used as a cyber weapon against Iran.
  - STUXNET: La primera ciberarma de la historia

www.EraDeLaInformacion.cl