E-ISSN 2014-0843
D.L.: B-8438-2012

opinión
Seguridad y Política Mundial

197
JUNE
2013

WHAT IF "THE MACHINE STOPS"? The need for a global cyber governance institution

Francesc Badia i Dalmases, Senior Fellow, CIDOB

Back in the year 2000, a PhD student innocently asked Manuel Castells, author of a reference trilogy on the digital age, the following question: "What about privacy on the Internet?" The answer came swift and clear-cut: "Forget about it!" the Open University of Catalonia scholar argued, "The Internet is an openly designed information-sharing system. If you try to lock it, you will kill it. The system, to be functional, must remain open and accessible from any given point of the network."

As a consequence of the IT revolution that took place during the last decades of the 20th century, a fully operative open information system was already up and running by the turn of the century, only to be captured by security intelligence services. And when in 2001 the 9/11 attacks occurred, and a surveillance state was put in place as part of the "war on terror" strategy, the old debate between freedom and security was set aside. Passing the Patriot Act and hunting Bin Laden and his Al-Qaida gang justified almost anything, including massive spying on fellow citizens.

The leaks of the 29-year-old intelligence contractor, Edward Snowden, to The Guardian and The Washington Post in early June revealed the existence of a Foreign Intelligence Surveillance Act (Fisa) order to American telecom behemoth Verizon. The company was asked by the National Security Agency (NSA) to deliver substantial data about calls of its 120 million customers. Government full access to massive data on telephone and e-mail traffic came to little surprise for the internet experts community, as did the revelations about the NSA's ability to siphon off any kind of digital information from the servers of major telecom and internet companies, including Apple, Facebook, Google, Microsoft, Skype, Twitter or Yahoo. There are legal limits to that, and Verizon only handed over "metadata" about connections but not access to content, which will require a specific order from the Fisa authority. But the fact is that, in today's highly interconnected world, anybody carrying a smartphone can be –and according to Mr. Snowden revelations a number of citizens currently are- tracked down by data-mining programs like NSA's Prism, used to monitor subscribers of main internet firms. Should security services be interested to read all your e-mails, see all your photographs, hear all your conversations and know your exact whereabouts, current technology can easily satisfy their curiosity. No real judiciary control takes place, Fisa rubber stamping is mere veneer: out of 34.000 requests since its inception, it refused only

11. Thus, in the name of cyber-security, core values of our open democratic society like the right of people to their privacy are being systematically violated.

The Internet infrastructure has become structural to our 21st century economy and society and, as professor Castells argued, has turn out to be to our economy what the electricity meant to the industrial revolution. Modern technology allows both intelligence bodies and commercial companies to monitor, at their caprice, our ideas, preferences, likes and phobias. Ultimately, in can be argued, it is Google or Facebook and not the government, who is spying on us. But if such thorough surveillance technologies are in place -and are being widely used, according to what we learned from the leaks, what the world is lacking is appropriate regulation bodies whose mandate and duty it would be to protect our rights as free citizens and consumers. The perils of abuse are evident, and the urgent need of a global cyber-governance institution that will have the legitimacy and the enforcing power to hold accountable those who violate peoples' rights has become obvious.

Strong reaction against this all out intrusion into privacy has followed in the world media, not only by civil society groups and cyber activists. After a dreadful lack of initial reactions from EU institutions even conservative lawmakers in the European Parliament backed a call for a clause to Europe's data-protection legislation, known as article 42. It would limit American Fisa authorisations to tapping international information traffic in the EU. But this might be somehow ineffective and have relative impact, since main data servers are physically based in US territory. Reinstating article 42 is a step in the right direction. No doubt. But, importantly, this is not enough to ease people's anxiety of an ever more intrusive Big Brother permanently watching all of us.

State cyber-security, particularly when it comes to counter-cyber-terrorism, is being widely discussed at international conferences and think tank rostrums all over the world.Less attention is being paid to the problems faced by lay citizens, who are seeing their rights to data protection and personal privacy threatened with little defence at reach. UN concerns about Human Rights implications of the Digital Age were showcased in a World Summit on the Information Society, convened in Geneva ten years ago. A special report was commissioned in 2011. It may be a good idea to build on these precedents and try to set in place an international authority able to protect people from being cyber-abused, and to regulate our digital age security flaws, that could become fatal sometime in the near future.

Our dependence on computers and communication systems is the measure of our fragility. The fact that our privacy is increasingly endangered is only a side effect of a much bigger problem: the 21st century economy and society relies heavily on openly interconnected computers: i.e. the Internet. The system is not immune to manipulations and failures. We have experienced some warnings that give us a glimpse of the magnitude of the breakdown if something goes definitely wrong at the "digital" level, such as "flash crashes" in the stock markets due to failures in the high-speed electronic trading systems, cyber-attacks to steal commercial, technological or military information, and computer viruses sent to disrupt nuclear facilities, as we saw with the Stutnex worm in Iran in September 2010.

Ahead from Huxley's "Brave New World" (1932), and Orwell's "1984" (1949), E.M. Forster wrote "The Machine Stops", a visionary short story that serves as a warning of the dystopia that could unfold, should our currently ungoverned digital space fall into major abuses and disruptions."But there came a day -the English author wrote in 1927-, when, without the slightest warning, without any previous hint of feebleness, the entire communication-system broke down, all over the world, and the world, as they understood it, ended". If our highly interconnected world, with all its virtues, is to be preserved, the international community must prevent that sort of dystopia from happening.