

Human Rights Council (UNHRC)

Combatting digital surveillance and data collection by authoritarian regimes

Santiago Fattoruso

**Forum:** Human Rights Council (UNHRC)

**Issue:** Combatting digital surveillance and data collection by authoritarian regimes

**Name:** Santiago Fattoruso

**Position:** Main Chair

**Introduction**

In recent years the digital world has seen an immense increase in its complexity and necessity. With people all over the world relying on digital technology to go on about their daily lives, the amount of data being used is growing drastically, and consequently so is the amount of monitorization and collection of this data. There is so much data being stored that it is practically impossible to keep track of all of it. This is why the surveillance and safeguarding of it is of global importance. However, the grand responsibility of watching over this data is often taken advantage of by authoritarian regimes, putting their nation and people at risk.

In these authoritarian regimes, the information they receive and store from digital activity is used for mass surveillance, data collection and censorship of what citizens may or may not do online. Often, the power that comes with this information is used for control instead of for protection. Entire lives of people are being stored away and processed without consent, stripping them away of their privacy and therefore their rights. They also

This lack of privacy is unacceptable and as members of the UNHCR, it is your responsibility to work together to find effective solutions on how to fight this problem, to debate on the extent of power of these authoritarian regimes over digital information, and to diplomatically reestablish a trustworthy and just system of digital surveillance.

This report will further elaborate on the extent of digital access authoritarian regimes have and the concerns it brings with it, the ongoing situation of misuse of this data, the many parties and factors involved with the issue at hand and what can be taken towards combatting this issue.

**Definition of key terms**

**Authoritarian regime**

System of government with a big concentration of power in a leader or group not lawfully responsible to the people.

**Digital surveillance**

The monitoring, recording and analysing of digital activities within an organization.

**Data collection**

The process of gathering, storing and measuring information.

**VPN**

A VPN (Virtual Private Network) is a system that allows users to use the internet securely and privately using encryption.

**General Overview**

The world which we live in depends highly on digital webs and systems. Without realizing it, people are handing over large amounts of data over to organizations in power, by making use of their digital devices. These organizations then have access to oceans of data, which they can then store, analyse and use in various ways. The access to this data has much potential for protection, technological and social improvement, and can be of great service to society. However, for authoritarian regimes, it is also an opportunity to gain control over the population, giving these regimes more power.

**Methods of data collection**

What makes this absolute control possible has to do with the constitutional structure of these authoritarian regimes. In these regimes there is no law nor constitution restricting how much data they receive. They also can create laws forcing the sharing of digital information, giving citizens no control over what is shared with the government. Think of signing up for services such as social media or banking apps which the government has access to, or the long and insufferable privacy policies of apps, which people often agree to without knowing what the policies include. Even allowing camera, microphone and location on your digital devices, gives regimes information to store and use for control over you. With so many methods of regimes receiving data, people are giving away much more of their privacy than they are aware of, and regimes never run out of information to use.

With all this input of information, authoritarian regimes have access to many aspects of people’s lives. They can use people’s internet activity to gain knowledge on their browsing history and IP addresses. With the rise of social media, they are granted access to posts, messages, and even deleted content. Mobile data includes people’s location, microphone, camera and calls. Even the digital identification system is used for the collection of medical, educational and financial information.

**Methods of digital surveillance**

The biggest reason for why this abundance of data available to authoritarian regimes is so dangerous, is because of what they can then do with the information to control the population. Firstly, they can create precise biometrics of individuals with the digital data. These biometrics can include facial, physical, and vocal recognition. This allows governments to be able to recognize any individual, leaving no room for privacy and secrecy. Another aspect of data collection is the vast databases that can be built with the information. These databases include everything, ranging from educational, financial and medical information, to storing people’s ID and SIM registrations to then be able to tie all online activity to their individuals.

Authoritarian regimes, having control over the digital interface, also gain the ability to control what the population can see and access on the internet. This allows them to be able to block the information the population receives and can therefore be crucial in manipulating the populations opinion, giving nation leaders immense power. An example of such a restricting system is the Great Firewall of China.

The Great Firewall of China is a regulatory and technological system of digital and internet control that the Chinese government uses to monitor, filter or block specific content for users within the nation. The firewall uses a filtering system of certain key words, blocks certain websites and apps, and blocks IP addresses from certain regions. By law, the Great Firewall blocks any kind of content offering political resistance and opinions against the Chinese government. It also blocks any information revealing state secrets and any content related to pornography, gambling and violence. The exact technical methods of the Great Firewall are only known to those who operate the system, but what is sure is that it has a massive effect on what not only the Chinese population sees, but also on the global population. These types of systems are what make controlling the population possible for authoritarian regimes and are therefore a threat to human rights.

Another one of these systems is Pegasus, a spyware system developed by the Israelian NSO group. This spyware is specialized in eavesdropping on mobile phones and collecting their data. This has already been used to track many politicians, government officials, human right activists and journalists. NSO claims that the software is only provided to the government and is only used to track dangerous individuals and to aid in rescue operations.

The effects of this data and digital control are therefore devastating. Firstly, people all around are losing their privacy. Near everything they do online can be collected, monitored and analysed by the government. Digital control also means that the population has a limited and selected extent of information they can get on the internet, controlled by the government, letting governments control what the population knows and therefore they’re opinion. This makes digital surveillance and data collection a tool for control over the population and an abolishment of the people’s privacy.

**Key Events Timeline**

**1998**  The project of the Great Firewall of China is started

**2011**  Pegasus Software is created

**31 March 2015**  Telecommunications operators in Russia required to install SORM equipment.

**2021**  United States Bureau of Industry and Security Sanctions NSO Group

**2022** Iran Internet Blackouts due to protests

**Principal Stakeholders**

**China**

China is the biggest example of a digital-authoritarian regime. The citizens of China no longer have the privacy they should rightfully have and their knowledge and opinion are in the hands of the Chinese government. For a major part this is due to the Great Firewall, the large digital databases they hold and the vast network of over 400 million surveillance cameras nationwide. These cameras are equipped with facial and vocal recognition, using them to feed information to the Chinese police. For example, in the Xingjiang province, every adult’s DNA, mobile phone data and iris scan are collected. They also have a mandated government app that uploads messages, calls and contacts, and an “Integrated Joint Operations Platform” which, with the help of AI, analyses all activity to then locate any suspicious activity. Chinese citizens try to resist by replacing banned keywords with synonyms and install certain available VPNs despite them not being allowed in the country, yet there isn’t much an individual can do against the Chinese system. To further increase their authoritarian control, the Chinese government sells software and technology involving digital surveillance, which are equipped with China’s restrictive digital governance rules, meaning that they not only are able to control the digital world inside their own nation, but also have influence abroad.

**Russia**

Under President Putin, Russia has been able to build an effective cyber-surveillance network. Since 2017, the Russian government has been installing surveillance cameras in public environments. Not only do these cameras damage their privacy, but they have also been used to track and catch participants in protests and enemies of the government. In regard to their internet surveillance, with their SORM system playing a major role in their digital control. This system intercepts interfaces of telecommunications and telephone networks operating in Russia. This includes calls, messages and any form of communication both from telephones and the internet, so banking transactions are also tracked. Just like China, Russia also works in filtering the internet, shaping the view of the population.

**Iran**

Iran is one of the biggest authoritarian regimes in the world. They’re most powerful tool is the isolated national intranet. This network has been operated so that thousands of foreign websites have been filtered and banned. The nation further influences the internet and digital networks by being able to shut them off at command. During protests they completely shut off the internet and mobile networks to prevent coordination and documentation during that period. They also regularly block social media apps, forcing Iranian citizens to use VPN’s, which are also mostly inaccessible due to them being banned. They even have mandated smartphone apps, like the Gershad app, which alerts woman of local police in the area who enforce hijabs.

**US Bureau of Industry and Security (BIS)**

BIS is a part of the United States government that regulates exports of sensitive technologies. They use economic sanctions to control the spread of surveillance tools and keep a database called the “Entity List”, with groups who engage in activities opposing the US’s view of national security. The BIS is crucial in control the spread of digital surveillance tools.

**Potential Avenues for Resolution**

**Strengthening human right laws**

One of the key solutions towards solving the issue at hand is strengthening human right laws. Currently these laws aren’t the same for all nations and allow authoritarian regimes to be able to act freely regarding digital surveillance and data control. These rights can be created regarding the amount of data governments are allowed to have access of the surveillance of the population with cameras and identification systems, and the controlling of the Internet. Delegates most work together to establish new laws regarding digital surveillance to strengthen the rights of people all over the world.

**Implementing export controls on surveillance technology**

Nations being able to sell their surveillance products over the entire world and share their knowledge on surveillance technology, makes developing a network of intrusive cameras and recognition systems easy for nations. That is why restricting or at least controlling the export of surveillance technology is vital in making sure that this digital-authoritarian way of governing doesn’t spread.

**References**

“Authoritarian.” *Merriam-Webster Dictionary*, 6 May 2025, [www.merriam-webster.com/dictionary/authoritarian](https://www.merriam-webster.com/dictionary/authoritarian).

Freedom House. “The Rise of Digital Authoritarianism.” *Freedom House*, freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

*GCSP Publication | Digital Authoritarianism: How Digital Technologies Can Empower Authoritarianism and Weaken Democracy*. [www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and](https://www.gcsp.ch/publications/digital-authoritarianism-how-digital-technologies-can-empower-authoritarianism-and).

P&Amp;RR. “Internet Shutdowns as a Tool of Authoritarian Repression.” *Politics and Rights Review*, 30 Mar. 2025, politicsrights.com/internet-shutdowns-authoritarian-repression.

Godfrey, Mary Kate. “How Autocrats Weaponize AI — and How to Fight Back | Journal of Democracy.” *Journal of Democracy*, 4 Mar. 2025, [www.journalofdemocracy.org/online-exclusive/how-autocrats-weaponize-ai-and-how-to-fight-back](https://www.journalofdemocracy.org/online-exclusive/how-autocrats-weaponize-ai-and-how-to-fight-back).

“China’s Techno-Authoritarianism Has Gone Global.” *Human Rights Watch*, 10 Nov. 2021, [www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global](https://www.hrw.org/news/2021/04/08/chinas-techno-authoritarianism-has-gone-global).

“Data Protection.” *European Data Protection Supervisor*, 13 May 2025, [www.edps.europa.eu/data-protection/data-protection\_en](https://www.edps.europa.eu/data-protection/data-protection_en).

Greengard, and Samuel. “Pegasus (Spyware) | Description, Origins, Spying, and Controversies.” *Encyclopedia Britannica*, 12 May 2025, [www.britannica.com/topic/Pegasus-spyware](https://www.britannica.com/topic/Pegasus-spyware).

“Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities.” *U.S. Department of Commerce*, 3 Nov. 2021, [www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list](https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list).

Wakefield, By Jane. *AI Emotion-detection Software Tested on Uyghurs*. 25 May 2021, [www.bbc.com/news/technology-57101248](https://www.bbc.com/news/technology-57101248).

McIntyre, Niamh, et al. “Online Gig Work Is Feeding Russia’s Surveillance Machine.” *TBIJ*, 5 June 2024, [www.thebureauinvestigates.com/stories/2024-03-27/online-gig-work-is-feeding-russias-surveillance-machine](https://www.thebureauinvestigates.com/stories/2024-03-27/online-gig-work-is-feeding-russias-surveillance-machine).

*China’s Great Firewall*. cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china\_policy.html.