HUMAN RIGHTS: Massive surveillance

"I do not want to live in a world where everything I say, everything I do, everything I speak, everything of creativity or love or friendship is recorded." – Edward Snowden

Advances in technological development allow people from all over the world to use the new information and communication technologies and, at the same time, increase the capacity of governments, companies and individuals to carry out surveillance, intervention and monitoring activities, data collection, which could constitute a violation or a violation of human rights, especially the right to privacy established in Article 12 of the Universal Declaration of Human Rights.

Massive surveillance occurs when authorities collect a large amount of information about the activity that a large number of people perform with their phones, computers or other smart devices.

In situations in which research files are presented regarding a crime and a certain person is considered suspicious of it, the authorities have the full power to investigate personal data that are held within the intelligent devices, so they make use of these means to collect evidence with the database they possess.

This means that if for some reason a person is attributed the character of suspect of a crime, the authority has the power to install cameras in front of their home or place of work and have access to their text messages and emails. This assumption is known as daily surveillance, which is directed to a specific person, as a suspect in a crime or terrorism.

Unlike daily surveillance, mass surveillance does not have a specific goal, and therefore can fall into a tracking surveillance.

These are situations in which a daily collection of data from a specific country on hundreds of millions of people, e-mails, phone calls, videos, photographs, records of website entries, and that data is revealed by a company of telephony or internet to security services, without the consent of the people affected.

Therefore, that mass surveillance means that nothing that is said on the phone, e-mails, text messages, photographs, videos, that is published on social networks, and nowhere to put the phone in your pockets, it is private.

The information and storage that you have on your computer, phones, tablets, can be tracked and stored by telephone companies/internet and security services without the consent of the affected person and specifically, without prior notice.

Edward Snowden's case

On June 5th, 2013, former CIA and NSA analyst Edward Snowden decided to reveal the existence of surveillance programs on the communications of millions of citizens around the world. Through The Guardian and The Washington Post, it was learned that, in the name of security and without any judicial control, the NSA and the British government that tracked e-mails, phone calls and encrypted messages. Companies such as Facebook, Google and Microsoft had been forced to deliver information about their costumers by secret orders from the NSA.

Snowden leaked to the press from Hong Kong and currently lives in Russia, where he was granted political asylum. He cannot return to the United States because he is accused of disclosing classified information to unauthorized persons and of theft of Federal Government property.

Massive surveillance is illegal according to international human rights instruments. Article 12 of the Universal Declaration of Human Rights enshrines it in Article 12, which says:

"No one will be object of arbitrary interference in his private life, family, home or correspondence, or attacks on his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks[2]."

As a result of this, the member States of the United Nations Organization have the duty to guarantee and respect the right of privacy in the context of digital communications, in such a way that only a judge can authorize interventions in private communications when they consider it strictly necessary, or when the law in addition to proving its effectiveness in preventing other violations of human rights.

---

[1] THE GUARDIAN. (2013) NSA Revelations. Guardian and Washington Post.

[2] United Nations (1948), DECLARAION UNIVERSAL DE LOS DERECHOS HUMANOS. Website: http://www.un.org/es/universal-declaration-human-rights/

Guided Questions:

1- How can governments guarantee the privacy of information and personal data to avoid exposing people to possible threats and dangers?
2- What other measure could the government use to monitor terrorist behavior of the citizens themselves?
3- What should be the limits of government towards the privacy of people?
4- What laws should be implemented for those who commit a misuse of technology and take advantage of information from people?
5- What kind of sanction would be given to people who violate the privacy of people?
6- What would be the limit of scope that people should have to technology?
7- What should be the restrictions for companies for the protection of personal data of their users?
8- What other human rights may be at risk of being violated with these practices?
9- How could the laws of protection to personal data be enforced in the Countries that do not regulate this assumption?
10- Has the use of mass espionage achieved improvements in terms of National Security, with respect to the protection of terrorism, or is it only an excuse for the State to have control and use personal data.

Research sources:

- The Universal Declaration of Human Rights (1948).
- Resolution approved by the General Assembly on December 18, 2013 68/167. The right to privacy in the digital age.
- American Declaration of Rights and Obligations of Man.
- ACTA. (Anti-Counterfeiting Trade Agreement).
- Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Council of Europe, 1981).
- Guidelines Governing the Protection of Privacy and Transportation of Personal Information (OECD, 1980).
- OECD (Organization for Economic Cooperation Covenant on Civil and Political and Development, Organization for Economic Co-Operation and Development).
- International Covenant on Civil and Political Rights.
- American Convention on Human Rights (Pact of San José).
- Privacy Conference 2009 (31st International Conference of Data Protection and Privacy Authorities).