ISSN: 2755-0133

Journal of Medical & Clinical Nursing

SCIENTIFIC Research and Community

Short Communication

Open Access

Security and Information Society

Tricia Bogossian

Specialist, Santa Úrsula University in Rio de Janeiro-RJ, Brazil

***Corresponding author**
Tricia Bogossian, Specialist, Santa Úrsula University in Rio deJaneiro-RJ, Brazil. E-mail: tricia.bogossian@hotmail.com

Received: April 19, 2022; **Accepted:** April 25, 2022; **Published:** May 23, 2022

Currently, the right to security is affirmed as a fundamental right in the most diverse legal and state systems. This is particularly observed in the Constitution of Brazil, which prescribes, in the wording of its article 5, that "All are equal before the law, without distinction of any nature, guaranteeing Brazilians and foreigners residing in the country the right to inviolability of the right to life, liberty, equality, security and property, in the following terms" (BRASIL, 1988, s.p.). It is noteworthy that in the aforementioned Constitution, the fundamental right to security is found in the chapter alluding to rights, freedoms and guarantees. It is also noted, for relevance, that the Brazilian legal system establishes the dignity of the human person as a fundamental principle of the Democratic State of Law. At the international level, it is possible to perceive the positivization of the fundamental right to security in several legal diplomas that catalog fundamental human rights. The Universal Declaration of Human Rights (UDHR), originating from the United Nations – the highest body for discussing International Law – states in its article 3 that "Everyone has the right to life, liberty and security of person". The same statement is reproduced in the International Covenant on Civil and Political Rights.

The consecration of the right to security as a universal human right is replicated in the other regional systems of International Law linked to the common axis of the United Nations. At the American level, the American Convention on Human Rights stands out – known as the Pact of San José de Costa Rica – which recognizes in its article 7, paragraph 1, first part, that "Everyone has the right to personal liberty and security ".There is no doubt, therefore, that security constitutes an inseparable end of the State – a teleological sense – which implies the guarantee of stability, permanence of Political Power and, therefore, associated with sovereignty. From this perspective, it denotes a duty of the State to institute instruments capable of achieving this objective.

When it released the Human Development Report in New York in 1994, the UNDP introduced, in Chapter Two of the Report, the UN's understanding of the idea, concept and approach around human security, electing seven central components that are interconnected and complete, in dynamic alignment processes to enable the potential of each individual in order to achieve their enrichment as a person. The seven central component spheres of human security contained in the aforementioned UNDP Report will be described below. Economic security aims at a secure basic income for people, usually from paid and productive work or, as a last resort, from a publicly funded safety net. While the issue of economic security is more serious in developing countries, it also raises concerns in developed countries. Unemployment and lack of income are important factors behind tensions involving political issues, crises or conflicts between ethnic groups (UNDP, 1994).

Food security requires that all people, at all times, have access, both physical and economic, to basic foods. There is no way to ignore the enormous unease with the lack of global availability of food for millions of poor people who are victimized not only by the deficient distribution of food, but also by the continuous lack of purchasing power (UNDP, 1994). Health security aims to ensure minimum protection in order to combat diseases and unhealthy lifestyles. Whether in developing or industrialized countries, damage to safety, in terms of health, is commonplace in urban and rural areas, particularly affecting needy children and the elderly with financial difficulties (UNDP, 1994).

Environmental security aims to protect people from threats and anthropic damage to nature, promoting the deterioration of the environment and harming environmental governance. In developing countries, the lack of access to environmental sanitation, such as clean water resources, sewage networks and solid waste treatment, constitutes one of the biggest nightmares of the human species in its habitat. In industrialized countries, one of the main problems is the atmospheric pollution that affects ecosystems. On the other hand, the growing impact of climate change is another burden that brings instability to environmental security and, consequently, harmful effects on human security (UNDP, 1994).

Citizen security is part of the context of human security, being the portrait of the protocol of public security policy for the valorization of human rights. It mobilizes the instruments of transformation, under the aegis of improving education, at the heart of the fight against violence and crime. Having as a priority pacification, the legitimacy of prevention alongside efficient police practice, citizen security aims to protect people from the afflictions arising from the threat of physical or moral violence, whether internally or externally. For many people, the biggest source of concern is the possibility of becoming victims of a violent crime at home, at school, at work, on the street, in sport, at leisure and, finally, in the virtual daily life of the Internet. The systematization of citizen security is the necessary path for social development with democratic governance (UNDP, 1994).

Community security involves ties of solidarity and social esteem with the philosophy and organizational strategy of partnerships between the population, governments and public and private institutions. This implies constant reforms and updates in planning, management and operationalization maps, respecting values, as well as ethnic and cultural identities (UNDP, 1994). Finally, political security is inherent to a society that respects the effectiveness of legal security, as a principle of legitimate confidence, in the exercise of power, which needs to be directed to the common good, taking care of guaranteeing the enforceability of the rules of law that motivate the harmonious relations between the State and the citizens (UNDP, 1994).

In addition to the multidisciplinary approach to security provided by UNDP, Arnold Wolfers, quoted by Luís Barroso (2014) uses two distinct dimensions – one of an objective nature and the other of a subjective nature. From these vectors, security is defined as the low probability of threats to the acquired values that simultaneously corresponds to the low probability of fear that these values may be attacked.

Certainly, in the current stage of complexity of social relations, of political, economic, social and cultural globalization, in which the geographic barriers of the States are increasingly decreasing, generating a migratory explosion in such a way that it transforms social coexistence into a "daily cosmopolitan", the risks and threats to which people and States themselves are exposed multiply in the same proportion. This is the phenomenon that Ulrich Beck (2011) called the "global risk society". With the advent of this information society, also called complex or risk society, doubts arise about the limits that can or should be imposed on public security bodies so that it is possible to contain crime. This is what will be discussed next.

Network and At Risk Society: Cyberspace, Privacy and Surveillance in Contemporary Society

According to the specialized literature, the information age is related to technological advances in communication and information in the digital field, starting in the 70s, with the invention of the computer, the internet and fiber optic cables. It is based on the process and dynamics of online communication, through networks, acquiring a multidimensional power, established according to the interests and values of different users (CASTELLS, 1999).In the 1980s, Alvin Toffler warned that the development of this entire technological process would also have serious side effects for society. Referring to espionage, in the context of the information and technology age, he expresses it as follows: [...] the spy agent is one of the most powerful metaphors of our time, as it is equipped with the latest and most exotic technology: electronic microphones, computer banks, infrared cameras, [...] espionage is information. And information has become perhaps the most important and fastest growing business in the world. The spy is a living symbol of the revolution that today invades the infosphere (TOFFLER, 1980, p.161-162).

Such a perspective, made in the years before the privatization of the internet, would be a harbinger of the moment in which we are currently living, characterized by a technological revolution punctuated by drastic changes in the way people perceive and act in their intimacy and private life. The spy agent Toffler was alluding to is cybernetic technology. Costa Júnior (2007) goes further when he states that the digital technological revolution promoted a process of erosion of the borders of intimacy, in which the invasion of private life became more acute and disturbing. He assesses that this revolution often advances without moral guidelines, which leads to a progressive deformation of fundamental rights on a scale of increasing harassment. Castells (1999), creator of the concept of network society, explains that we are connected to groups of people with distinct interests and unlimited access, which we can understand as networks. Basically, these are open, integrative and dynamic structures, with unlimited expansion capacity, where people share the same communication codes to access or share their information.

The author explains that this phenomenon is the result of the interaction of two relatively autonomous forces: the development of new technologies and the attempt by society to re-equip itself "with the use of the power of technology to serve the technology of power" (CASTELLS, 1999, p. .69). In this context, it is important to remember that, in these networks, the conventional hierarchy and the identity of the users become insignificant. From the perspective of Souza and Quandt (2008), the most striking aspect is the position in which these identities are found within the network itself, with the respective contacts and peripheral nodes, often more important than being located at a certain hierarchical level, even higher.

Using the same method of analyzing peripheral contacts to identify connections and leadership between criminal organizations, governments can exercise surveillance by constantly monitoring these nodes. Fellman and Wright (2008), dealing with the theme by clarifying that the measurement of these networks is focused on their degree of centrality, reveal the key individuals in the flow of information and in the exchange of knowledge. High degrees of centrality demonstrate broad access to hidden resources within the organization. Thus, after the identification has been carried out, surveillance works to make it possible to point out other contacts around this one and, gradually, add new connections until the complete mapping of which people are leaders and with whom they are involved. It is in this sense that Castells (2013) claims that interactivity is one of the factors that transform these networks into decisive sources for building a portion of power, but not all power. It is relevant to say that the internet, conceived as a product of the Cold War in the late 1950s, was essentially characterized as a military research project prepared by the Advanced Research Projects Agency (ARPA) at the request of the United States Department of Defense, designed to connect US research centers with the Pentagon, providing opportunities for the exchange of secure information between these centers. In the lesson of Castells (2003), the creation of the internet was also a consequence of the dispute for superiority in military technology with the Soviets, creating a communication channel and safe storage of scientific data, in case of nuclear war, which at the time, in fact, it was a real possibility.

On the other hand, the history of the internet is permeated with successes and setbacks in a long process. Briefly, in 1971, a team of scientists, led by Vinton Cerf, considered the father of the internet, had accomplished the feat of connecting three different networks in a process called interneting, a term that later came to designate the system that today is known as the internet. . With the creation of a new network specifically for military communications, the Military Network (MIL-NET), in 1983, the Advanced Research Projects Agency Network (ARPANET) lost its exclusivity in this area (NETHER, 2018). In the 1990s, under the control of the National Sciense Foundation (NCF) and with the collaboration of the Department of Defense, the internet would be commercialized to other governmental institutions and the private sector. With the inclusion of TCP/IP protocols and the WWW (World Wide Web) system, developed by Tim Berners-Lee, it would be privatized from the 1990s onwards, reaching users in this way (NETHER, 2018).

The structural model of internet governance is centered on the US Department of Commerce and Defense, which has military control of cyberspace, ICANN (Internet Corporation for Assigned Names and Numbers) and the company Verising, which has, with exclusivity, commercial control. It is worth mentioning that, according to the magazine Em Discussão (2014), "the two companies are responsible for assigning internet protocol parameters, using the regulation of the domain name system, for the allocation of blocks of IP address numbers and for the system root server management". Simultaneously, the term cyberspace began to be referred to, as will be detailed below.

Cyberspace, cybersurveillance and cyberespionage

Working on the concept of cyberspace is significant for the present study, as it is in this metaphysical environment that virtual threats of different types occur, including cybersurveillance and cyberespionage. Synonymous words are usually used to define it, such as virtual space, virtual world and electronic realm. However, it is known that the expression originated in science fiction, coined by the English writer in the work Neuromancer, by William Gibson, released in 1984, being immediately incorporated into the digital language. The author's contribution becomes of great value, as he referred to cyberspace as a field of struggles and conflicts within the scope of digital networks, in the search for secret information protected by programs, which would lead to new economic and cultural frontiers, a conjuncture that presents itself today.

The US Summary National Strategy to Secure Cyberspace of 2003-NSSC defines it as hundreds of thousands of networked computers, including internet, intranet, and telecommunications networks, servers, routers, and fiber optic cables that enable the operation of critical structures. Pierre Levy (1999) contributes when he presents a broader concept of cyberspace and includes human beings as an active part of this system. He asserts that it is a global information infrastructure over the Internet, integrated by the universe of data that circulates through it and by the users, scientists, technicians and other specialists responsible for its maintenance and development. Libicki (2009) goes even further, adding that cyberspace is divided into three levels: physical, syntactic and semantic, and it is within one of these levels that cybersurveillance and cyberespionage actions are developed.

The physical level is where all information systems are located in a physical layer that supports them and are made up of boxes and wires. In turn, the syntactic level contains instructions that program creators and users give to the machine, as well as the protocols through which machines interact in the machine.
Writer who inaugurated the so-called "Cyberpunk Era", where he anticipated technologies such as the internet and created the concept of "cyberspace" in the 1970s (NETHER, 2018, p.69). data elaboration, device recognition and document formatting. It is at this level that hackers tend to operate. Finally, the semantic level consists of information that machines contain and that different types of attacks occur on them, through viruses and websites with embedded malicious codes (LIBICKI, 2009).

Based on this scientific dimension, it is possible to identify that it is at the syntactic and semantic levels that cybersurveillance and cyberespionage activities occur, since they are the ones that enable access to data and information. However, according to Nether (2018) the internet can be considered only a small portion of communication on the Web. There is another segment to which there is no easy access, known as the Deep Web, which is a virtual, non-indexed environment that criminal organizations, digital pirates and terrorist groups easily gravitate to, counting on the technical and operational difficulties of effective monitoring. Indeed, it is on the Deep Web that a significant portion of government monitoring is concentrated, carried out through their intelligence and defense agencies, in order to anticipate risks and threats. This action occurs by analyzing the nodes of connections to the network and creating fake profiles. The biggest problem is that its pages and sites, such as those of terrorist, pedophilia and drug trafficking networks, do not remain accessible for a long time, being systematically replaced. In a globalized world, in which we seek to access vast amounts of information in a timely manner, cyberspace constitutes a critical dimension of the normal functioning of modern society, its security, its economy, its business (IDN, 2013). This dimension provides opportunities for new and growing types of cyber threats, a fact that has led countries that dominate cybernetic technology to use it with a broader spectrum, initially, as a legitimate defense against various suspicions that threaten national security. But also, for the indiscriminate collection of information and personal data aimed at different interests for unknown people. In view of the historical synopsis presented, it is necessary to mention two points that had not yet been mentioned. The first concerns the discovery made by Bob Thomas, the worm called The Creeper. At the time, it wasn't considered as such, as this concept did not yet exist, being treated as an experimental self-replicating program. Thomas aimed to demonstrate that there were vulnerabilities in the machine's security system and, for that, he sent an unauthorized message containing the following expressions: "Im the creeper, catch me if you can" "I am the creeper, catch me if you can." able" (KLEINA, 2020).

The second was the discovery of spam in 1979. It was disseminated in the form of mass e-mails, inadvertently created by Digital Equipment Corporation (DEC), which intended to launch a commercial product in the North American market and, for this purpose, sent a series of of marketing messages that flooded the net. These two findings are quite significant, as they made it possible to verify that the recently created system had vulnerabilities, characterized by the possibility of access by unauthorized users and imperceptibly, to any type of data and information, a context that has evolved to the same extent in that new programs and systems are being developed. According to the Internet Security Glossary, vulnerability is defined as any weakness or weakness in an equipment or system, which can be exploited by one or more threats. They may be intentional or the result of design errors that result in unwanted or unintended effects that compromise system security. The ones that bring the greatest risks are those unknown by the manufacturer or system manager and, consequently, there are no mitigation mechanisms that make it possible to protect the network perimeter until the identification and development of new hardware or software.This broader dynamic points to technological platforms, such as cloud services, social networks and mobile technologies, such as Tablets, Smartphones and the Black Berry, which have offered the malicious user a new door to exploit their attacks (IDN , 2013).

Wendt (2011), using Caverty's studies, identifies five types of threats presented in ascending order, according to the motivation and potential of the risk. Etymologically, the terms are preceded by the word cyber or the English expression cyber, which internationally expresses any type of communication that takes place in the digital space. Norton. Internet security glossary. Available at: http://br.norton. com/security-glossary/article. The first threat is named by the author of Cybervandalism, characterized by the actions of hackers, motivated by challenges, jokes or contempt. A classic example is the replacement of part of a website's content with other unauthorized content, usually of a pornographic or personally offensive nature. The second is Cybercrime, whose motivation goes beyond the simple challenge and triggers some type of damage protected in the criminal sphere. Among a variety of cases, one can cite the capture of credit card passwords aimed at carrying out bank fraud, distributing pornographic material and violating intellectual property. In Cyberespionage, the specific motivations are aimed at obtaining commercial, industrial and governmental secrets. In Cyberterrorism, attacks that target critical structures of a region or country, capable of causing collapse in basic services threatening the integrity of a country. The first case of cyberterrorism occurred in 2007, in Estonia, where several basic services to the population were temporarily paralyzed, causing several inconveniences to the country.

Finally, there is cyberwar when it affects the sovereignty of the nation through attacks on computers linked to the adversary's critical infrastructure, such as energy, water and transport networks, health services, causing the destruction of systems and their permanent paralysis.It is necessary to point out that, both in the classification mentioned above and in various studies, cybersurveillance is not included as a threat, it is not even mentioned. This stems, in part, from two aspects. First: more in-depth studies on the consequences of cyber-surveillance are recent and still poorly understood by users of the World Wide Web in general. Second: the lack of knowledge regarding the functioning and technological capabilities of the internet.

As Lemos (2016) adds, understanding technology, its strengths and limitations should be a fundamental component of global citizenship. This is equivalent to saying that, not understanding how it works, users, most of the time, do not realize that they are being monitored and, when realize, they do not have an exact idea of how such non-consensual action will impact their lives. Reinforcing this perception, the Kaspery laboratory disclosed the existence of an international cyberespionage campaign called Red October, aimed at collecting data and information from organizations, governments, diplomatic agencies and research and technology centers, all considered sensitive and protected by a degree of secrecy. regarding access (VELOSO, 2014). As a result, other related episodes came to the attention of the international media, as was the case of the British spy agency, Government Communications Headquarters (GCHQ), which, together with the NSA, began to tap communications carried out through fiber optic cables. , including phone calls and messages sent via emails in the UK.

The evidence, of a documentary nature, also pointed to the close collaboration of private companies in providing personal data to these governments. Nevertheless, it can be said, based on the general knowledge about this technology, that both episodes brought to light new and broad reflections, namely: the definitive overthrow of the myth of the utopian inviolability of cyberspace and its alleged character of privacy, which allows users to pay extra attention to the content they post and access; an international alert in the sense of the need for constant improvement of technological means, to guarantee the secrecy of its confidential documents and the protection of information and personal data; and the demonstration of the breadth, scope and complexity of the government cyber-espionage network that relies on the direct collaboration of private companies, in addition to the public exposure that it entails in the countries and citizens targeted by these activities (COLLI, 2010). In this logic, the arguments exposed above contribute to elucidate, in part, the reasons for the reticence of those who develop and hold cybernetic technology in sharing it, or even the difficulties in regulating it, as an instrument of control and power.