SPECPOL

(Committee on special policies and decolonization)

Monitoring of public and private information acquired and manipulated by the government

&

The impact of fake news on the democracy

Index

1 Introduction to the committee

1.1 History

The Special Committee on Politics and Decolonization (SPECPOL), also known as the United Nations Fourth Commission, was created in 1993 in accordance with General Assembly Resolution 47/233 . Prior to 1993, until its 48th session, under the name of the Decolonization Committee, the Fourth Committee was solely responsible for matters related to trusts and decolonization. However, after independence was granted to all

the United Nations Trusts and the trusteeship system was dismantled, the commission's workload and cases to be dealt with decreased dramatically. Consequently, the Decolonization Committee was merged into the Special Political Committee, previously created as a seventh main committee, to form the current Special Committee on Policy and Decolonization (SPECPOL). Mainly, SPECPOL was created taking into account the declarations by the United Nations, which named the new decade of 1990 as, "The international decade of the eradication of colonialism," 1 with the aim of the extermination of the colonies to turn them into States. sovereigns. During this time, 750 million people lived on colonized lands, highlighting the need to create the new commission. In its inception, the main objective of SPECPOL was to address, debate and resolve important political issues that the First Committee (Disarmament and Security - DISEC) could not deal with. These political issues included issues such as self-determination, decolonization, and other international security issues.

At present, the Fourth Committee “deals with a wide range of issues: five issues related to decolonization, the effects of atomic radiation, issues relating to public information, a comprehensive examination of the issue of maintenance operations of peace, as well as that of the special political missions, the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), the report of the Special Committee in charge of Investigating Israeli Practices and International Cooperation in the Peaceful Uses of Outer Space. "

In addition to this, SPECPOL can be seen as “the gateway” to the United Nations Security Council, taking into account that the problems discussed in the Security Council are previously evaluated by the General Assembly through SPECPOL, thanks to its broad approach. in terms of international

security. Furthermore, unlike other bodies, SPECPOL allows the participation of all UN member states, which generates a broad and diverse evaluation of the issues.

Among its general aspects, the power of SPECPOL is stipulated in Chapter XI of the United Nations Charter, where the commission's main objective is to commit to taking care of the rights of those individuals who live in a colonized territory.

Currently, the 193 member states of the UN are part of SPECPOL and have a voice and vote within the commission. With this in mind, its resolutions are not binding, but they are very attractive to the international community, as they reflect the opinion of the majority on substantive matters. On the other hand, the Fourth Commission meets annually from the end of September to mid-November. In addition, it meets briefly in the spring to adopt the peacekeeping-related resolutions and decisions approved by the Special Committee on Peacekeeping Operations .

1.2 Purpose

SPECPOL, like all United Nations committees, has the purpose of enforcing human rights, specifically in cases of decolonization, atomic radiation and public information. Your goal is to keep the peace. It focuses on the Middle East region, where it has had several special operations such as, the United Nations Relief and Works Agency for Palestine Refugees in the Near East; Furthermore, its general objective is to protect the rights of the inhabitants of the colonized territories. This commission is in charge of special political missions that take part mainly in Africa, Asia and South America, diplomatic missions with a focus on human rights.

In addition to colonization on planet earth, SPECPOL deals with colonization and the peaceful use of outer space, mining and the Universidad Para la Paz, an educational organization of the United Nations located in Costa Rica. All these approaches are intended to monitor the implementation of human rights and United Nations regulations in vulnerable territories and communities, as well as control political resources to ensure their proper use.

This committee has three main objectives: the elimination of non-autonomous territories; the search for solutions in the form of treaties regarding humanitarian and political problems, such as decolonization; and the guarantee of security for territories with a history of colonization.

1.3 Challenges and problems solved

Although SPECPOL cannot pass immediate resolutions, the commission is responsible of all world affairs regarding decolonization, special political missions, peacekeeping operations, and the protection of war refugees, among others. Therefore, the Fourth Committee is responsible for passing resolutions on how the member states of the United Nations should deal with these problems, which has had great positive repercussions worldwide. As the main challenge resolved by SPECPOL, the number of people living in colonized territories affected by violence and suppression has dropped from 750 million to an approximate of two million, since the creation of the UN. This is the greatest achievement of the Fourth Commission, taking into account that it was created precisely to exterminate the colonies worldwide and turn them into sovereign States. The United Nations, through SPECPOL, has succeeded in providing independence to more than 80 nations, which are currently sovereign countries. On the other hand, SPECPOL's hard work has

contributed to the maintenance of world peace and security. Through the creation of 69 peacekeeping and observation missions in different conflict zones of the world during the last 10 decades, the United Nations, thanks to the work of SPECPOL, has been able to restore calm in many areas of the planet. With this in mind, peacekeeping missions have enabled many countries to recover from conflict situations. In actuality there are 16 peacekeeping operations deployed in different parts of the world, involving 112,000 people from 115 countries.

Similarly, in terms of peacemaking, since the 1990s, SPECPOL's mediation efforts, together with the activities of third parties, have contributed to ending numerous conflicts. These include the conflicts in Sierra Leone, Liberia, Burundi, and the north-south conflict in Sudan and Nepal. According to research studies, UN peacemaking and conflict prevention activities have reduced conflicts in the world by 40% since the 1990s. Furthermore, actions by SPECPOL have succeeded in defusing many potential conflicts. On the other hand, the 14 United Nations peace missions on the ground deal with post-conflict situations and implement peace-building measures.

Although SPECPOL's global work is mostly seen on the issues of decolonization and peacekeeping, the Fourth Committee has also managed to influence the prevention of nuclear proliferation, the fight against terrorism, the promotion of human rights, the development of Africa and the provision of humanitarian aid to refugees.

1.4 Relevant figures and information about the committee

Working Methods:
The fourth committee of the General Assembly, SPECPOL, has an annual meeting that begins in September and runs through mid-November. Also, they meet in the spring to make decisions on the treaties passed by the Special Committee on Operations for the Peace-keeping. These meetings have delegates from the 193 countries belonging to the United Nations. On his agenda, every two years, are issues related to mining and, every three years, with the University of La Paz. During its sessions, SPECPOL has openings for civilians and affected people to present themselves and present their position on colonization.

Directors:
The following make up the bureau of the Fourth Committee for the 75th Session of the General Assembly:

Name	Country	Position
H.E. Collen Vixen Kelapile	Botswana	Chairperson
Darren Camilleri	Malta	Vice-Chair
Paul Hussar	Romania	Vice-Chair
José Osvaldo Sanabria Rivarola	Paraguay	Vice-Chair
Jassim Sayar A. J. Al-Maawda	Qatar	Rapporteur

Reporting Bodies:
The following organisms report to SPECPOL:

- Information Committee
- Committee on the Peaceful Use of Outer Space

● Special Committee on Peacekeeping Operations
● Special Committee on Decolonization
● Special Committee for the Investigation of Israeli Practices Affecting the Palestinian People and Other Arabs from Occupied Territories
● United Nations Relief and Works Agency for Palestine Refugees in the Near East
● United Nations Scientific Committee on the Effects of Atomic Radiation

Resolutions:

Annually, the committee passes around 30-35 resolutions. Resolutions regarding Israeli practices, Palestine and some decolonization resolutions are passed by popular vote. SPECPOL resolutions are generally negotiated first and then presented. When the draft text is related to the work of a subsidiary body, the presiding Member State of the subsidiary body facilitates negotiations. Delegates co-sponsor draft resolutions electronically through the e-deleGATE portal.

2 Monitoring of public and private information acquired and manipulated by the government.

2.1 Introduction to the topic

Monitoring the use of the Internet, cameras with facial recognition, and other measures that governments take to monitor their citizens, are considered by many to be invasions of privacy.

In several countries, specifically China, the use of advanced surveillance cameras implemented by the government is becoming popular. The Chinese government has already installed more than 170 million cameras with facial recognition in its country, as well as video cameras that have artificial intelligence capable of recognizing individuals from their way of walking. The excessive use of these devices has caused panic among citizens, who they fear for their privacy.

In addition to cameras, several countries are using Unmanned Aerial Vehicles (UAVs), or drones, to try to improve security. The US government began to use Unmanned Aerial Vehicles in its police investigations, a fact that has worried several news networks, saying that they can be used to invade the privacy of the innocent. Using this technology could track a person's movements. They will know if they attend demonstrations and protests and where they were. Most of the Unmanned Aerial Vehicles used by the United States have a camera called the DJI Zenmuse Z30 , a device with a total focus of 180x, which allows spying from thousands of meters away. This makes it capable of identifying individuals and license plates with ease. Unmanned Aerial Vehicles are significantly cheaper than other tools used by the police, such as helicopters. For the cost of a helicopter, they can purchase 500 Unmanned Aerial Vehicles, which are stealthier and more discreet. One of the most common models among the police is the Inspire 2 , which costs around $ 3,000, adding the DJI Zenmuse Z30 camera , which has the same price, the total cost is $ 6,000 dollars, while a helicopter has a cost between $ 500,000 and $ 3,000,000 dollars.

This technology has proven to be useful for investigations at a distance or in inaccessible places; likewise, it prevents the risk of human lives in cases of fires and natural disasters. Although they have a great benefit, it is necessary to implement limitations to protect the privacy of citizens. Spying and invasions of privacy aren't just physical. Many governments have been accused of creating systems to monitor the electronic devices of their citizens. The United States, France, the United Kingdom, and China are some that have had scandals of this type of espionage. With systems like PRISM, created by the US National Security Agency, they can interfere with text messages, calls, and information shared over the Internet. Companies such as Google, Yahoo, Facebook, Microsoft, and Apple have been blamed for sharing their users' private information with various governments, yet they voraciously deny it.

With all the information that the government receives, there is another question: the information that it distributes. The traditional media have been modernized with the technological advances of the last decades. With sites such as Facebook, Instagram and Twitter, which open up communication possibilities that did not previously exist, the disclosure of information was facilitated, even if it was not true. Fake, or misinformed, news is the modern aspect of tabloid journalism: outrageous and emotional news made to capture the public's information regardless of whether it is informed or true. The creation of legislation to limit this fake news is necessary; however, monitoring public information is strictly against the right to freedom of expression and information.

Fake news is not the only problem. On several occasions, governments ask to limit the information that reaches the public from the media.

After the September 11 attacks on the Twin Towers, the US government asked several newspapers, including The New York Times, to first report to the White House before publishing information on the attacks. They refused to please. The request was made to prevent mass panic and danger. Governments withhold national information ensuring that it is for the safety of the people. They think that, in addition to causing panic, they can be a threat to national security, since information in the wrong hands can be dangerous.

2.2 Key concepts (Terms)

1. Monitor: Control the development of an action or an event through one or more monitors.

2. Privacy: The ability of an individual or group to isolate themselves, or information about themselves, and thereby selectively express themselves. The boundaries and content of what is considered private differ between cultures and individuals.

3. Digital privacy: The protection of an individual's information that is used or created while using the Internet on a personal computer or device.

    a. Information privacy: The notion that people should have the freedom or right to determine how their digital information is collected and used, mainly that related to personally identifiable information.

    b. Communication privacy: The notion that individuals should have the freedom or right to communicate information digitally with the expectation that their communications are

secure; which means that messages and communications will only be accessible to the original recipient of the sender.

c. Individual privacy: The notion that people have the right to exist freely on the Internet, in the sense that they can choose what type of information they are exposed to.

4. Public data: Information compiled by the government. These include DMV (Department of Vehicles) records, vital statistics, professional licenses, voter registration, assessor and registrar documents, etc.

5. Public information: Information that is already a matter of public record or knowledge. With regard to government and private organizations, any member of the public can request access or disclosure of such information, and there are often formal processes in place for how to do so.

6. Private information: Private data of an individual, particularly in relation to the Internet. This information should not be accessed by anyone else without the consent of the individual.

7. Voluntary information: Information voluntarily provided by a user on the web. (Ex: social networks, phone numbers)

8. User Generated Content (UGC): Any form of content, such as images, videos, text, and audio, that users have posted on online platforms such as social media and wikis.

9. Classified information: Information subject to special security classification regulations imposed by many national governments, the disclosure of which may harm national interests and security.

10. Censorship: The suppression of speech, public communication or other information, on the basis that such material is considered harmful, sensitive or "inconvenient." It can be conducted by governments, private institutions, or corporations.

11. Prior Restriction: A type of censorship in which speech or expression is reviewed and restricted before it occurs. Under prior restriction, a government or authority controls what speech or expression can be publicly released.

12. FOI (Freedom of Information): Freedom of information. The right of a citizen to access the information held by the state. In many countries, this freedom is supported as a constitutional right.

13. Surveillance: Monitoring behavior, activities, or information for the purpose of influencing, managing, or directing.

14. Drone: An aerial vehicle that flies without a crew, also known as an Unmanned Aerial Vehicle (UAV).

15. Cyber espionage: A form of cyber attack that steals classified confidential data or intellectual property to gain an advantage over a competitive company or government entity.

16. Artificial intelligence: An area of computing that emphasizes the creation of intelligent machines that work and react like humans.

17. Noticias Falsas (“Fake News”): Tabloid journalism that consists of deliberate misinformation or deception, spread through the traditional media or on social media online.

18. WWW (World Wide Web): An information space where documents and other resources on the web are identified. All resources and users on the Internet that use the Hypertext Transfer Protocol (HTTP).

19. LAN (Local Area Network): Local area network. A computer network that interconnects computers within a limited area, such as a residence, school, laboratory, college campus, or office building.

20. WAN (Wide Area Network): Wide Area Network. A telecommunications network that extends over a large geographic area.

21. VPN (Virtual Private Network): Virtual Private Network. A computer network technology that enables a secure extension of the local area network (LAN) over a public or uncontrolled network such as the Internet.

22. NSA (National Security Agency): The United States National Security Agency. A nationwide intelligence agency of the United States Department of Defense, under the authority of the Director of National Intelligence.

23. PRISM (Preemptive Reconnaissance and Identification Security Mainframe): Preventive Recognition and Central Security Identification. A codename for a program under which the United States National Security Agency (NSA) collects internet communications from various internet companies in the United States.

24. CIA (Central Intelligence Agency): The Central Intelligence Agency is a civil service of foreign intelligence of the federal government of the United States, in charge of collecting, processing and analyzing national security information from around the world, mainly through the use of human intelligence.

25. US Fourth Amendment: Protects the right to privacy and the right to be free from arbitrary invasion.

26. Physical surveillance: The monitoring of activities and behaviors using physical methods (cameras, drones, etc.)

2.3 Deepening the topic

2.3.1 Historical background

The technology needed for this type of spying and invasion of privacy is recent. Cameras with facial recognition, Unmanned Aerial Vehicles and electronic device monitoring systems are innovations of the last decades.

For this reason, the historical antecedents correspond to the 21st century.

In 2008 Edward Snowden, an employee of the United States Central Intelligence Agency revealed the use of PRISM, a system used to acquire the information of citizens by monitoring their private online conversations and more, by the National Security Agency . PRISM is an acronym for Preemptive Reconnaissance and Identification Security Mainframe, or Preventive Recognition and Central Security Identification. Several companies, such as Google, Yahoo, Facebook, Apple and Microsoft, were accused of providing that information. The heads of Those companies have declared their innocence, with Google and Yahoo declaring that they only provide personal information when they receive legal orders for a specific individual. Ensuring that this program is for the defense and security of the country, the United States government says it is to protect itself from possible attacks by illegal groups and cybercrime. On the other hand, the Court of Justice of the European Union started Schrems II , a case that aims to prohibit the transmission of private information from the European Union to the United States by companies. Although the European Union, specifically Finland, is against these practices, they have discovered several European countries with their own version of PRISM.

A French newspaper, Le Monde discovered that, "The Director General of External Security systematically collects the electromagnetic signals emitted by computers and telephones in France ... All our emails, SMS, telephone records, accesses to Facebook, Twitter, are saved for years."

This report included the same information providers as PRISM: Facebook, Yahoo, Apple, Microsoft, and Google. The National Information and Freedom Commission does not allow these programs, but it also claims to be within the law. The UK also takes part in this surveillance, the Communications Headquarters, or GCHQ, spying on its citizens and foreigners. This program is called Tempora; the British government neither confirms nor denies its existence. Likewise, Russia has also been accused of participating in cyber surveillance. For fear that their government will acquire their information, many citizens have turned to VPNs, a Virtual Private Network, to defend their privacy. Chinese citizens have shown fear because of the facial recognition cameras that their government has set up to monitor their people.

The system of more than 170 million cameras, 12 for every Chinese citizen (implemented by the government) has the power to recognize and distinguish one face out of millions. In addition to this, they developed an artificial intelligence that can discern the person from their way of walking and body shape.

Adding to these cameras are Unmanned Aerial Vehicles, message surveillance, video cameras and more. WeChat, the most popular messaging platform in China, has a penetration rate of around 83%, and in 2018, the anti-corruption Communist party's watchdog revealed the acquisition of deleted messages from WeChat.

Additionally, they began to implement special hats that detect brain wave changes in workers in industrial zones, in the military and in high-speed train drivers. These devices can perceive emotional changes and determine stress levels to modify work and rest times, an effort to

increase their level of production. One company, State Grid Zhejiang Electric Power, used this solution and resulted in a profit increase of 2 billion renminbi (315 millions of dollars). The investigations of this product, called Neuro Cap, are located at Ningbo University in China. This project is founding by the Chinese government. The device, which looks like a safety helmet, was received with distrust and resistance from the workers. Research for Neuro Cap continue, hoping to

perfect the instrument. North Korea is one of the countries with the longest history of abuse of the privacy of its citizens. The government has absolute control of the communications of its people.

They monitor your calls and all uses of electronic devices. Besides espionage Excessive cybernetics, control of the media and information directly violates human rights. The only way to connect to the Internet in North Korea is by its domestic Internet site, known as Kwangmyong , which is only allowed to view content previously approved by the government. External news or propaganda alternative to that of Kim Jong-Un is strictly prohibited. Violating these laws and communicating with the outside world is cause for being committed to prison camps. To try to escape this oppression, Korean citizens resort to transporting Chinese cell phones as contraband. In Colombia, its political Constitution stipulates “all people have the right to their personal privacy… and to rectify the information that has been collected about them… in files of public and private entities,”

2.3.2 Present situation

Today, government manipulation of public and private information poses a threat to Internet freedom and is leading the rise of global digital authoritarianism, particularly led by China. Disinformation and propaganda spread online have poisoned the public sphere. The collection of personal data by the government has destroyed traditional notions of privacy. Hence, a large number of countries are moving towards digital authoritarianism by adopting the Chinese model of extensive censorship and automated surveillance systems.

As a result of these trends, global Internet freedom declined for the eighth year in a row in 2018. As an example of this, several events related to Internet scandals emerged in 2018. First, in April 2018, the founder and CEO of Facebook, Mark Zuckerberg, testified in two hearings in the United States Congress on the

His company's role in the Cambridge Analytica scandal, which revealed that Facebook had exposed the data of up to 87 million users to political exploitation. On the other hand, Russian hackers attacked American voter rolls in various states as part of the Kremlin's efforts to weaken the integrity of the 2016 elections. Since this scandal, security researchers have discovered new data breaches affecting 198 million Americans, 93 million Mexicans, 55 million Filipinos, and 50 million of Turkish voters. As democratic societies grapple with the challenges posed by the internet and social media, leaders in China have intensified the use of social media, digital media to increase your power, both within your own country and internationally. For example, over the past year, the Chinese government hosted officials from multiple countries for two- and three-week seminars to discuss its extensive system of censorship and surveillance.

In addition, its companies have supplied telecommunications hardware, advanced technology facial recognition, and data analysis tools to a variety of governments with poor human rights records, which could benefit Chinese intelligence services as well as repressive local authorities. With all this in mind, it is clear that digital authoritarianism is currently being promoted as a way for people to Governments control their citizens through technology, which presents an existential threat to the future of the open Internet.

Internet controls in China reached new extremes in 2018 with the implementation of the Cyber Security Law and updates to surveillance technology. The law: centralizes all Internet policies

within the China Cyberspace Administration (CAC); strengthens the obligations of network operators and social media companies to register users with their real names; requires local and foreign companies to work to, "immediately stop broadcasting" of prohibited content; and obliges them to ensure that all data about Chinese users is hosted within the country. Additionally, authorities have cracked down on the use of VPNs to bypass the Great Firewall, prompting Apple to remove hundreds of the services from its local app store. As an advocate for cybersecurity in China, there is President Xi Jinping who, speaking in the Chinese Communist Party Congress in October 2017 publicly outlined its plan to transform China into a "cyber superpower." He also offered the country's governance model, including its management of the Internet, as, "a new option for other countries and nations that want to accelerate their development while preserving their independence."

As an example of the Chinese dominance over its citizens is the System in Service Social. In 2014, the Chinese government announced a social credit system, in which citizens will receive grades and scores for their behavior. Misconduct in public, such as playing loud music or crossing the street as a pedestrian when it is not due, can result in not being able to buy a plane or train ticket. Because of this system, 169 Chinese citizens are prohibited from flying for crimes such as delays in paying debts and misconduct on past flights. Systems similar to these have existed in the past by private companies. This Chinese system is the first government controlled, although it has not reached national levels yet. Currently, local governments have their own version, with their own criteria. China aims to have a national version of the credit system by 2020. The blacklist is part of the credit system social credits. An individual is added to the blacklist when he commits a crime such as owing money to the government. Liu Hu, a Chinese journalist, was added to the list when reporting on government corruption and censorship. Being blacklisted, you are prohibited from buying plane and train tickets, property, or receiving a loan.

Hu commented: “There was no file, police order or prior official notification. They just banned me to things to which he was previously entitled. "

To properly track Internet freedom around the world, Freedom on the Net conducts an annual survey of Internet freedom in 65 countries around the world, covering 87% of the world's Internet users. In 2018, this study revealed that of the 65 countries evaluated, 26 have had an overall decline since June 2017, compared to 19 that recorded net improvements. The largest decline in scores occurred in Egypt and Sri Lanka, followed by Cambodia, Kenya, Nigeria, the Philippines, and Venezuela.

An example of this decline is the event suffered by two women in Egypt, who were arrested in separate incidents for uploading confessional videos on Facebook.

to report sexual abuse in that country. Both women were accused of spreading false information to harm public safety. On the other hand, in Sri Lanka, authorities closed social media platforms for two days during communal riots that they erupted in March, causing at least two deaths. In the same study conducted by Freedom on the Net, it was found that in almost half of the countries where Internet freedom declined, the reductions were related to elections. Twelve countries suffered an increase in disinformation, censorship, technical attacks, or arrests of government critics in the run-up to the elections. For example, during the presidential elections in Venezuela in May 2018, the government passed a law that imposed severe prison sentences for inciting "hatred" online. In addition, the implementation of the "Tarjeta de la Patria", an electronic identification system used to

channel social assistance, raised suspicions that the data collected through the device could be used to monitor and pressure voters.

On the other hand, in Cambodia, ahead of the general elections in July 2018, the country saw an increase in arrests and prison sentences for online speech as the government sought to expand the number of crimes used to silence dissent. , including a new law against them majesty that prohibits insults to the monarchy. On the side of Kenya also he went from "Free" to "Partly Free" in the study, manipulation and misinformation online influenced voters during the elections of August 2017, while a law CyberCrime adopted in May of 2018 increased the maximum penalty for posting "false" or "fictitious" information to 10 years in prison.

Regarding the situation in the United States, the study indicates that Internet freedom in this country also decreased. The Federal Communications Commission revoked the rules that guaranteed net neutrality. This move sparked efforts by civil society groups and authorities at the state level to restore protections at the local level. In a blow to advocates of civil rights and privacy, Congress reauthorized the Act Amendments of FISA, including Section 702, thus losing the opportunity to reform the surveillance powers that allow the government to conduct broad searches of personal information. Despite an online environment that remains diverse and free, misinformation and hyperpartisan content continue to be an urgent concern in the United States, particularly in the run-up to the 2020 elections.

On the positive side, of the 19 countries with improvements in the overall score, two, Armenia and the Gambia, had improvements in their Internet freedom status. Armenia went from “Partially Free” to “Free” after citizens successfully used social media platforms, communication apps and live streaming services to bring about political change in the country's Velvet Revolution in April. On the other hand, the Gambia went from “Not Free” to “Partially Free”, as restrictions have been eased and users have been able to publish content more freely since the dictator, Yahya Jammeh, was forced to leave office to early 2017.

As for fake news, the term “fake news” has been adopted by authoritarian leaders to justify measures against the opposition. Deliberately falsified or misleading content is a genuine problem, but some governments are using it as a pretext to consolidate their control over the information. Last year, at least 17 countries passed or proposed laws that restricted online media as a fight against "fake news." Several governments are turning to the regulation of users of social networks as means of communication to legitimize new repressive measures against online speech. For example, Egypt passed new legislation that requires all social media users with more than 5,000 followers to obtain a license from the Higher Council for Media Regulation. This measure is similar to laws passed in countries such as Cambodia, China and Russia. Similarly, many governments are imposing criminal penalties for publishing what they consider to be fake news. In 2018, 13 countries, including Bangladesh, Rwanda, Kazakhstan and the Philippines, prosecuted citizens for spreading false information. Considering the level of global Internet freedom, it is evident that more governments are turning to China for guidance and support at one point in which the global leadership of the United States is in decline. Hence, in this aspect of global Chinese dominance, digital authoritarianism will become an inescapable reality almost by default. Furthermore, in an increasingly globalized and technological world, governments, private companies, and researchers are increasingly hungry for vast amounts of personal information, being used for purposes ranging from political repression to the development of artificial intelligence algorithms. . Taking this into account, so far, ordinary citizens tend to have few options to resist this acquisition of information by higher entities.

2.3.3 Measures implemented to solve the problem

To prevent the spread of false news, several organizations have been born, created by joint ventures between citizens, governments and companies. In Brazil, the Association of Investigative Journalists affiliated with Primer Draft (First Draft), to create Comprava, an organization that gathers 24 news companies to correct false information about the elections.

Similarly, Chequeando is an Argentine organization that has a system to compare news with truthful information to ensure that what the public receives is real. Furthermore, Facebook collaborated with DFRLab and discovered several fake accounts created in Iran and Russia.

At the international level, there are no measures to prevent the circulation of news false and limiting the media. Laws are needed for abuse of the monitoring of these media, as can be seen in North Korea. Privacy International is a London-based non-profit institution that aims to protect people's privacy internationally. It seeks to confront governments and companies that have dishonored the privacy, dignity and freedom of people to confront them in legal proceedings. They initiate investigations to incriminate guilty entities and to achieve institutional changes in legislation to increase the security of private information. Part of its scope is to inform about the dangers of government surveillance and ways to prevent it. Between reports, campaigns and news, they seek to prevent invasions of privacy to civilians. Adding to international efforts to limit cyber espionage, the United Nations International Telecommunications Union established the Global Cyber Security Index, which measures countries' level of commitment to security in electronic devices and Internet use.

In response to fears about the constant collection and insecurity of personal data, many countries are enacting laws that give individuals the right to control how their data is collected, processed, and shared by public and private entities. At least 15 countries have considered data protection laws since June 2017, and at least 35 already have a data protection law. The data protection laws that have been proposed or passed in Argentina, Brazil and Indonesia bear a strong resemblance to the EU General Data Protection Regulation (GDPR), which came into effect in May 2018.

This regulation requires data subjects to obtain more meaningful consent, increasing transparency about what data is collected and why. Additionally, it provides a way for users to download, transfer, or delete their information.

However, the regulation does not apply to matters of national security and defense, so it cannot restrict the rampant collection of governments. Despite this, the GDPR is one of the most ambitious attempts to regulate data collection in the 21st century.

In the United States, several states have passed or proposed laws to increase media literacy programs in local schools. Civic education initiatives include efforts to teach students to assess the credibility of online media sources and identify misinformation. This measure is very important to combat the manipulation of information, since people are adequately informed about how to use networks and the Internet. Similarly, WhatsApp, owned by Facebook, is working together with seven organizations in India to develop a digital literacy training program for its users.

Finally, an innovative national model can be found in Estonia to solve the current problem. Its platform, X-Road, for the secure exchange of data, runs on a local blockchain called KSI, through which all incoming and outgoing transactions are authenticated and encrypted. Among other benefits, citizens are notified when government agencies access their data files, except in cases of

ongoing investigations. Given Estonia's strong legal framework for privacy rights, the system provides greater protection than in countries where citizens' data is stored unencrypted on disparate servers, with no mechanism to inform them about who owns the information or how it is being done. using. Therefore, in 2018, Estonia announced plans to expand the X-Road platform internationally.

2.3.4 Future expectations

For the future, information manipulation and cyber espionage by of governments increases, taking into account the development of new technologies and the probable global influence that China's Internet control model could have. In addition, it will increase the desire of governments to protect and access certain information to ensure their national security as threats, such as attacks by illegal groups, increase. Hand in hand with this are hackers, who also increased with the progress of technology, creating a greater need for encrypted and protected information by governments.

In the first instance, as China strives to become a power of artificial intelligence by 2030, the moral and ethical concerns surrounding technology deserve further attention. Like nuclear science, artificial intelligence (AI) will inevitably fall into the hands of governments seeking to use it for authoritarian purposes. Democracies around the world will also face temptations, considering the attractive use that AI applications can have, from electronic commerce to national security. Therefore, ensuring that government agencies and private companies comply with ethical codes will require constant vigilance by civil society, investigative journalists, and official oversight bodies. On the other hand, as the influence of technology increases, it is essential that citizens take action and hold companies and governments accountable for their unethical measures and actions. As an example of this are the actions taken by 1,400 Google employees in August 2018, who in an internal letter from the company called for greater transparency after media reports revealed plans to launch a censored mobile news and search service. in China, where user activity would be linked to their phone numbers. Similar internal pressure in June led the company to reevaluate its work with the United States Department of Defense in the field of artificial intelligence and led to the president executive, Sundar Pichai, to publicly promise that he would not seek to implement artificial intelligence applications. However, although citizen influence and the guarantee of practices Ethics on the part of governments can have a role in reducing the misuse of surveillance technologies, the best way for democracies to stop the development of digital authoritarianism is to demonstrate that there is a better model to manage the Internet. This means addressing social media manipulation and data misuse in a way that respects human rights, and preserves an Internet that is global, free, and secure.

In addition, it is essential to develop a digital education system in all countries of the world to ensure good use of social networks and the Internet in general. Democratic governments will have to devote far more diplomatic and other resources to counter China's offensive on the international stage. An essential part of this is fostering collaboration between civil society groups, governments and technology companies to achieve protection of the digital sphere and avoid manipulation. If democracies fail to promote their own principles and interests with equal determination, by default, digital authoritarianism will become an inescapable reality.

Finally, to protect citizens' information, it will also be essential to include suitable legislation that gives people the right to control how their data is collected, processed and shared by public and private entities. Currently, at least 15 countries have considered data protection laws since June 2017, and at least 35 already have a data protection law on the books. However, these laws are not

perfect, since the regulations do not apply to matters of national security and defense, so it cannot be restrict rampant data collection by governments.

Therefore, in the future, regulations suitable for all actors in society must be created. Governments and technology companies should strive to increase transparency regarding how personal data is used, allow data portability between platforms, and allow individuals to review and delete all data collected about them - steps that some of the The world's largest companies have already taken.

According to Freedom on the Net, these are some measures that should be taken in the future to improve the situation of the global Internet:

For politicians:

● Make sure that all laws and practices related to the Internet are

adhere to international human rights laws and standards.

● Enact strict data protection laws to provide greater transparency and control over personal data.

● Fund rapid response capacity to counter attacks on Internet freedom.

● Impose sanctions on foreign technology companies involved in human rights abuses.

For the private sector:

● Adhere to the UN Guiding Principles on Business and Human Rights .

● Conduct human rights impact assessments for new markets and commit to doing no harm.

● Give users control over their information and make sure it is not being misused.

● Ensure fair and transparent content moderation practices.

● Participate in an ongoing dialogue with local civil society organizations.

For civil society:

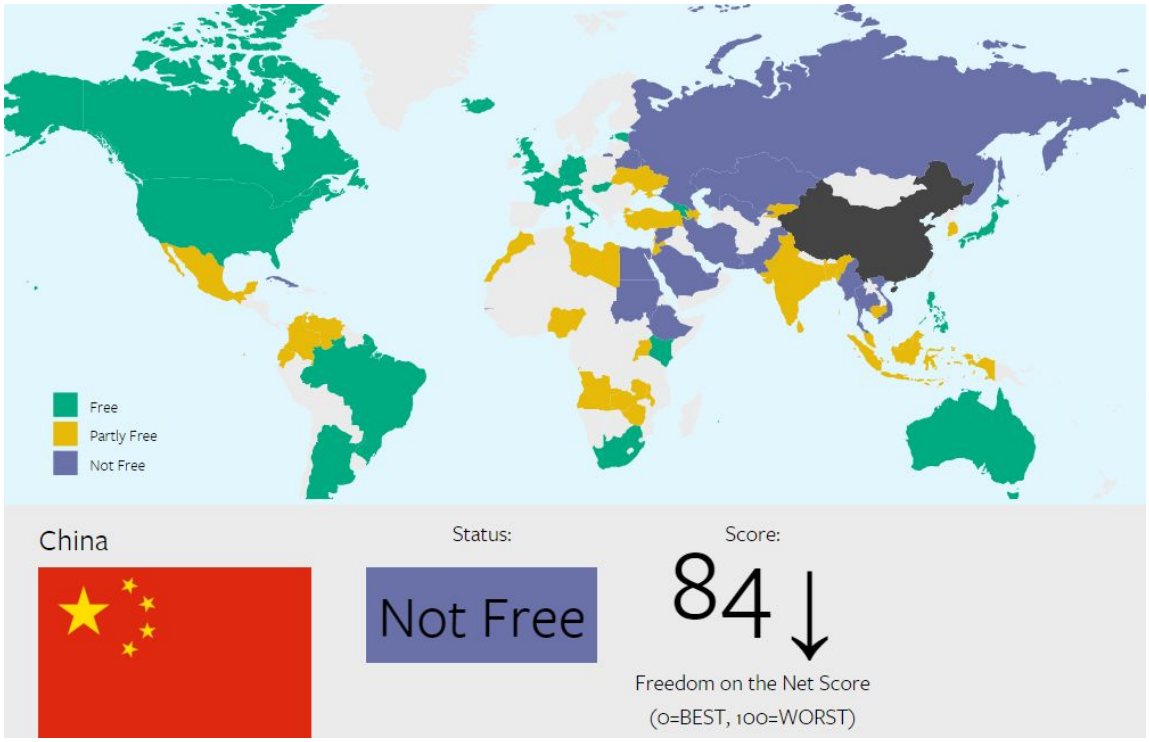
● Partner with the private sector in fact-checking efforts.

● Work with academics to examine how misinformation spreads

● Continue to raise awareness of government censorship and surveillance efforts.

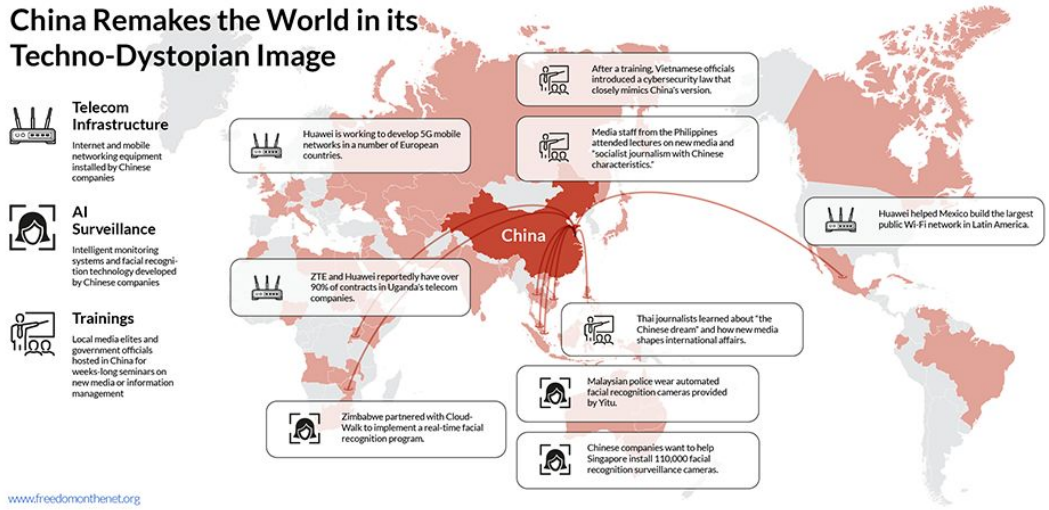
2.3.5 Other aid

Source: Freedom House



State of internet freedom in countries of the world

- Green: Free
- Yellow: Partially Free
- Purple: Not free



Where your Privacy Is (and Isn't) Protected

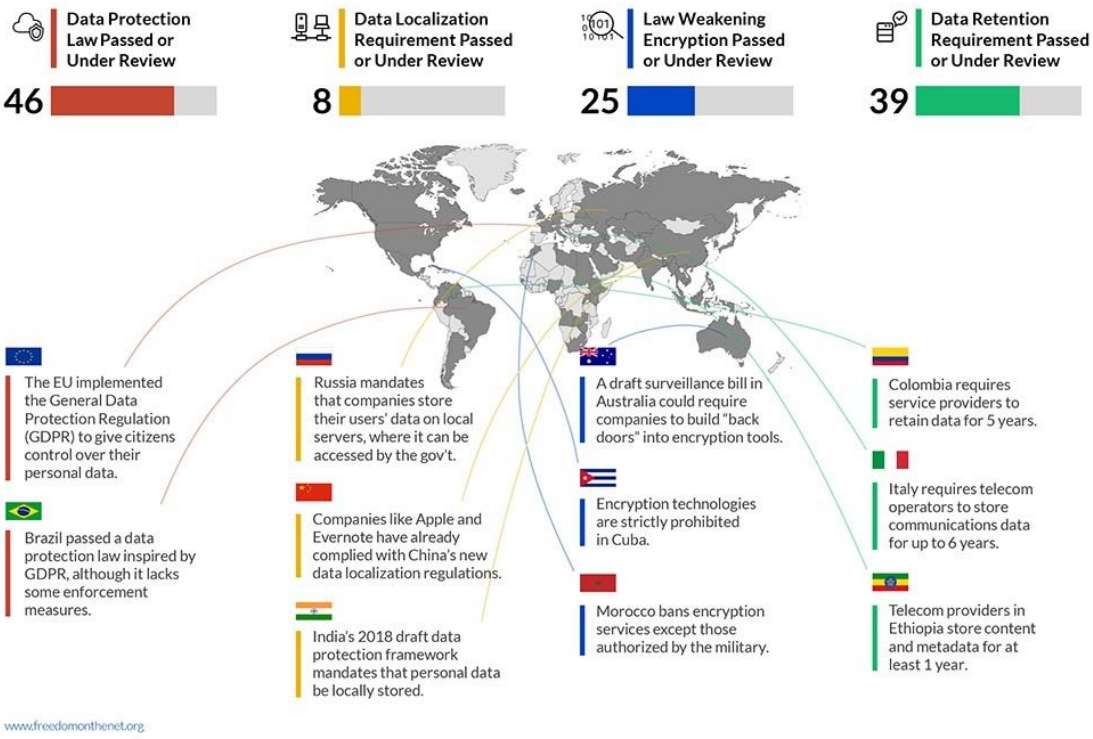
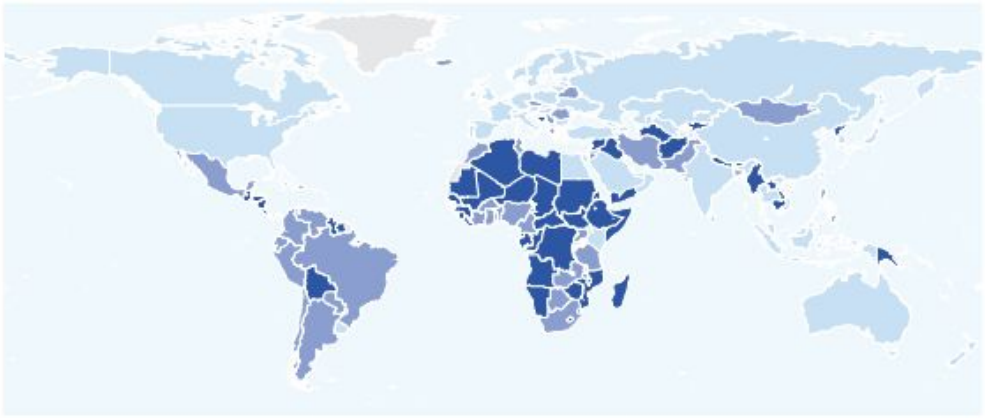


Figure 4: Heat map showing geographical commitment around the world



The colours in the heat map above indicate differences in the level of commitment with high, medium, and low scores in a range of colours from light blue (peak commitment) to dark blue (low commitment). This is also reflected in the GCI groups in section 4.2.

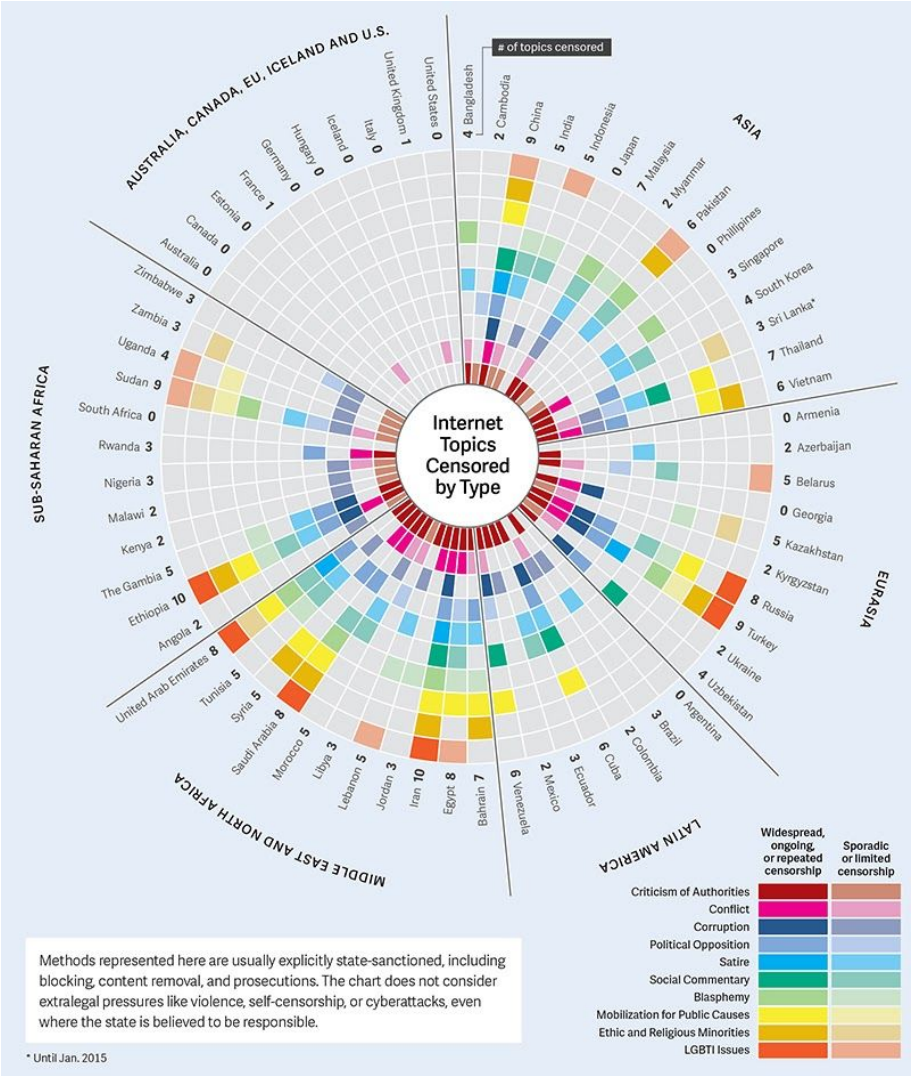
4.2 GCI groups

Countries are classified according to their level of commitment: high, medium, and low.

1. Countries that demonstrate high commitment in all five pillars of the index.
2. Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives.
3. Countries that have started to initiate commitments in cybersecurity.

Freedom House

www.freedomonthenet.org



2.3.6 Useful questions for your position paper

1. What are the measures taken by the government of your country to monitor its citizens (physical and cyber surveillance)? How have these measures been received by the population?

2. Does your country have Unmanned Aerial Vehicles in its police forces? If the answer is yes, in what quantities are they used and what laws do they have to prevent their abuse?

3. What laws does your country have in relation to the handling of citizens' personal data?

4. How are the relations between the government of your country and companies regarding private information of citizens?

5. How did your country react to the global cyber espionage scandals (eg, PRISM revelation by Edward Snowden)?

6. What is the level of Internet freedom in your country? How is this level of freedom related to your country's system of government?

7. What laws does your country have to monitor and limit the media to prevent “fake news”? What has been the public response to these measures?

8. Has your country suffered from scandals related to the manipulation of information by the government / private companies? If yes, how were the scandals handled?

3 The impact of fake news on the democracy

3.1 Definition of the problem

3.1.1 History

In 2016, Donald Trump used the term fake news to accuse journalists who criticized his presidency, popularizing the term internationally. Despite the fact that advances in technology - understood as the level of accessibility for users, personalization and global reach - have had a clear impact on the proliferation of the concept of fake news , this term and the facts to which it refers have existed since long before.

Before the printing press was invented, the main generating entities of fake news were the States, through the minting of engraved coins, and the churches, which gave speeches from a position of power. An example of this is given in 44 BC, when Octavian handed out coins with slogans against Mark Antony. The coins bore short phrases that insulted Mark Antony as a womanizer, drunkard, and puppet of Cleopatra.

In 1450, when Guttenberg invented the printing press, the dissemination of information, such as news or books, was democratized and popularized. That is the same impact it had on disinformation, which was only generated by States, but private entities also played a role in its production and dissemination. "The Great Deception of the Moon" (1835) was the first false news written, which was created by the New York Sun newspaper and proposed that life had been discovered on the moon.

The wars of the 20th century presented clear examples of the use of fake news in the printing press. In World War I (1914-1918) propaganda was used to encourage recruitment in several participating countries. In the United States, the Woodrow Wilson government created the Committee on Public Information (CPI), whose role was to manage information about the war in the country. Thus, they focused on the newspapers publishing only positive news about the war (ignoring disasters and defeats), with the aim of recruiting American soldiers. On the other hand, the Daily Mail and the Times of England published a story about Germany, which argued that, as a result of the English blockade, the German government had built a corpse factory, where they burned the bodies of soldiers to generate fat and food for pigs. The Second World War was characterized by Nazi propaganda, led by Goebbles and his Ministry of Propaganda and Public Education, which was in charge of transmitting messages of hatred and violence against the Jewish community. This was not only a clear example of the use of fake news to spread violence and exacerbate the division of society, but it also put the State, once again, as an actor and generator of disinformation.

Other wars that were linked to the generation of fake news were those of Vietnam (1955 - 1975) and Iraq (2003 - 2011). In the first, the US government used the domino theory - which argued that if one country embraced communism, all would follow - to generate terror and win support in the war. On the other hand, the conflict in Iraq showed that fake news does not only involve Western actors. The New York Times published a series of reports on the production of biological weapons of mass destruction in Iraq, which prompted the invasion of Iraq by the US government. On the other hand, Muhammed Saeed al Sahhaf was an Iraqi diplomat who proclaimed false news about the conflict, such as denying on television the presence of enemy tanks in Baghdad, which were circulating behind him in the recording.

In the mid-1980s, advances in technology that until then were only used by researchers, professionals or the military, finally entered the commercialization phase. In 1989, the Englishman Tim Berners-Lee created an international system of protocols that allowed network users to execute and send documents in a standard format. The World Wide Web (WWW) was created and with it the URLs (Uniform Source Location or web page), HTTP (Hypertext Transfer Protocol) and HTML (Hypertext Markup Language): its use continues to this day and allows the generation of texts, images and animations in an international network. This has created a new platform of rapid transmission and difficult regulation, which is used to generate and spread viral content that contains fake news today.

Currently, the presence of journalists in the digital sphere is almost inevitable. The technological revolution impacted the traditional media, with a drop in advertising revenue and the capture of an audience whose main information medium is "peer to peer."

The introduction to the online world by traditional media has led them to take an immediate behavior, where data review and editing processes are increasingly scarce, which impacts the quality of the news and the veracity of the information. . This milestone promoted the generation and dissemination of fake news ,

On the other hand, technology has enhanced fake news by allowing the interaction of individuals and organizations - both the media and the state - from various nations. Although the main conflicts in the relationship between the internet, technology and social networks will be analyzed in the following sections in detail, some relevant events of recent years will be explained below.

Organizations specialized in generating fake news had their first appearance in 2014, when workers from the Internet Research Agency confessed that they were paid to enter forums to post anti-Western and pro-Kremlin messages. The Internet Research Agency , a Russian agency dedicated to the spread of online disinformation and the use of armies of trolls, hired workers who had 6 fake Facebook accounts and 10 Twitter accounts, publishing between 5 posts and 50 tweets to audiences of 500 and 2000 subscribers. Between 2016 and 2017, for-profit companies were discovered in Veles, Macedonia, considered “ trol farms ” or cyber trolling farms , which generated viral content for different North American political parties and used advertising platforms such as Google Ad Sense to carry out follow-ups to your speeches. Finally, Cambridge Analytical (2018) used data from online profiles to create micro-focused political messages, which are not only expected to be shared by the user but also create a greater division between positions and perspectives of the truth.

All of these organizations and individuals have had a clear impact on polls and elections around the world. From the 2016 elections in the United States - where thousands of fake American accounts were created -, or Brexit - with its disproportionate number of pro-separation users on Instagram -, to the presidential elections in several Latin American countries which were hacked by a team led

by the Colombian Andrés Sepúlveda: all these events have been impacted by the opportunities offered by social networks and the massive commercialization of the internet.

3.1.2 Definition of fake news: options and variants

Fake news is a term that comprises a series of definitions and sub-terms that make it up, which must be understood before its causes, implications and possible solutions can be analyzed.

The news fake currently exist in an era of post - truth , which is understood as an era dominated not facts but emotions, beliefs and desires of the public. Thus, the Oxford dictionary further specifies that the latter are more relevant in shaping public opinion than the same scientific or proven facts.

Following this contextual definition, we can approach the different variants of the fake news concept , which are preliminarily explained by UNESCO. It is necessary to differentiate the fake news from the news or classic journalism . While the second has a professional and ethical character - although not lacking in narrative and perspective - any form of fake news lacks such attributes. According to UNESCO, weak or problematic journalism, which is a consequence of a lack of investigation or sensationalism, also differs from fake news.

What do we understand then by fake news ? One possibility is to consider it as disinformation , which is false information, intentionally spread by an issuer who knows its falsehood.

UNESCO also adds the term “ misinformation ” that can be understood as disinformation that does not contain the intentional element: it is false information that the issuer believes to be true, and likewise spreads. In any case, it could be understood that "misinformation" is the consequence of an initial (intentional) misinformation, which is disclosed and creates convinced recipients who republish the information. In terms of intent, information with intent to harm can also be considered - where some hate speech, harassment and other categories would fall in.

Another relevant aspect, whose membership is not fully established, is the relationship between fake news and social networks. Is fake news a phenomenon limited to the digital medium? Can we also consider them outside of these? The Journal of Internet Law defines fake news as the intentional online publication of false statements of fact. However, print media and media individuals can also generate intentionally false content. Would they then be fake news ?

Finally, it is interesting to note the physical characteristics of fake news , since these often consider a format and content identical to that of official media - which is created with the intention that published news have greater credibility. This is another aspect to consider when formulating possible definitions of fake news , which goes beyond the content itself, but the design and presentation possibilities it has.

3.2 Discussion of the problem

3.2.1 Regulation of fake news

In the West, social networks operate in a scenario that has been described as "legal exceptionality." With few exceptions, companies are not responsible for the content that runs through their digital platforms. The reason why social networks have been outside the regulation of the States is because, for the Law, they have remained as simple intermediaries without responsibility for the content of the information. However, very recently, States have begun to become aware of the consequences of fake news on democracy and the rights of their citizens.

In May of this year, Singapore became the latest state to pass anti-fake news legislation . Parliament passed a bill put forward by the government called Protection from Online Falsehoods and Manipulation Bil . The government justified the initiative by claiming that it is necessary to protect citizens from fake news and educate them about the potential harm they have, in particular about incitement to racial and religious violence. Under this rule, the government itself would be in charge of determining the veracity of the information. In case of finding false information about public institutions, the government may issue corrections that must be published and, in extreme cases, may order digital platforms to remove certain content. Likewise, the norm provides criminal penalties for those who are declared responsible for publishing falsehoods with malicious intent. In this regard, Facebook and Google pointed out that, although they support the regulation of fake news , they are concerned about certain elements of the draft regulation, such as the use of vague terms without specific definition such as "public trust."

However, there are already a number of States with regulations in force that punish or regulate disinformation on digital platforms: Bangladesh (2018), Belarus (2018), Cambodia (2018), Egypt (2018), France (2018), Kenya (2018)), Malaysia (2018), Tanzania (2018), Thailand (2018) and Vietnam (2019).

The approval of these laws, however, has not been free of opposition and controversy on the political scene. In the case of France, for example, the draft rule proposed by President Emmanuel Macron was rejected by the Senate twice before being approved.

Likewise, other countries have draft legislation traveling the legislative routes in their respective jurisdictions: Brazil, Chile, India, Ireland, Russia, South Korea, Sri Lanka and Taiwan. The option of Germany and Croatia, for their part, was to address hate speech on social networks and propose the responsibility of digital platforms in eliminating them.

Although all these norms or proposed norms seek to regulate the formation and dissemination of fake news , they do so in different ways. The most common is to use Administrative Law and Criminal Law to punish, through fines or limitations on personal freedom, those who spread false information on social networks. However, most of these measures are designed to criminalize the mastermind of such information and fail to effectively address the role of digital platforms in its dissemination and availability. Likewise, many of the regulations provide the power of the government to block certain information that it considers dangerous.

However, although they have not developed and issued specific regulations, disinformation has taken center stage in the political sphere. Many countries have taken action in this regard, among which we find the formation of committees to investigate or evaluate the current situation: Australia, Belgium, Brazil, Canada, Democratic Republic of the Congo, Denmark, Italy, the Netherlands, Nigeria, Pakistan, Korea from the South, Spain, Sri Lanka, Sweden, Turkey, the United Kingdom and the United States. These organizations or ad-hoc investigations have achieved positive results in clarifying facts and responsibilities, as well as proposals to address this problem.

For example, in the United States, the Special Council to monitor the investigation into possible Russian interference in the 2016 presidential elections produced a report whose content has been crucial to American democracy.

In other countries, arrests, investigations and criminal proceedings have been registered based on standards of domestic legal systems, such as those referring to national security or fraud: Bahrain, Benin, Cameroon, China, Ivory Coast, India, Indonesia, Italy, Myanmar, Rwanda, and Saudi Arabia. However, it should be noted that this situation could represent a danger to freedom of expression and of the press, in which the government can control the information available to the public from its political interests.

3.2.2 Freedom of expression and the media

The Universal Declaration of Human Rights establishes that everyone has the right to freedom of opinion and expression, including the right to maintain an opinion without interference, and to seek, receive and impart information and ideas through any means of dissemination without limitation. of borders. The freedom of the press, the creation of independent media and the presence of journalism are all promoters and enjoy the rights stipulated by it. However, in the rise of fake news , they are suffering limitations, reduction and even harassment, since they represent many values (ethics, professionalism, truthfulness) that disinformation is trying to bring down.

According to the Inter-American Commission on Human Rights, as of 2017, more than 10 percent of the cases of violence against journalists and communicators in America were committed through digital platforms, which occurred “through various forms of improper access to accounts in social networks and databases and actions aimed at preventing the availability of pages and services on the web ”.

The news fake not only stifle journalistic content for greater range and penetration can have, but in some cases even directly impact the lives of journalists. For example, in 2017 Mexican accounts of trolls were used to influence the referendum in Catalonia, voting against independence and resulting in a high level of polarization and aggression towards journalists.

They have also managed, through their hate speech and conflict, that journalists suffer death threats and even have to flee the country.

The consequences are mainly psychological: although the journalist does not decide to act against them by blocking or responding to the comment, he is still affected by the insults. Furthermore, it is a cumulative process, in which journalists themselves, as a result of harassment, decide to be less present online or even change their profession. According to the Council of Europe, of the total number of journalists attacked by fake news , 31 percent reduce coverage of the issue, 15 percent stop dealing with it and 57 percent do not report the violence. This means a decrease in your exercise of freedom to express what you want, in the medium you want.

However, there have also been clear attacks, most frequently against women and researchers. One particular case was against Nadia Daam, a French journalist, who accused in a radio program that trolls from the Forum BlaBla 18-25 had intercepted an anti-bullying helpline. After this criticism,

the journalist was threatened with death, her emails were hacked and posted to pornographic sites, and she even received phone calls. His harassers were charged and sentenced to suspended prison.

The news fake not only affect journalism indirectly. The term fake news has been used against the traditional press, with the aim of delegitimizing and despising it, as well as to be able to impose various regulations to control it. This has been done mainly by the same governments or political representatives who accuse journalists and media who criticize their proposals or have a point of view different from their own of publishing “ fake news ”. Beyond the Trump case, probably the best known, it has been identified that, in 2017, 21 journalists were jailed for the offense of publishing “ fake news ”, 10 of them Egyptians and 9 Turks. These acts constitute a danger to freedom of expression and pose a conflict between what each State considers to be public safety - or potential harm to society - and freedom.

In addition to regulations directed at technology companies or social networks, as explained in the previous section, States are beginning to regulate journalists, whether they are generators of online or offline content . The main problem with this type of regulation is the subjectivity on which the decision is made, being the State who decides if the news is considered as fake news or not. Taking the previously mentioned example of Singapore, the government enforces the legislation based on what it considers to be a threat to public safety and the state, which can be used to censor any journalist who makes an unwelcome comment or criticism. Using a term as broad as “the best interests of the state” or “public safety” is an imminent threat since it can be applied to many types of expression.

3.3 Fake news as a political tool

The news fake have been strategically used by candidates for public office to manipulate information or presenting it. However, the signifier " fake news " has also been used as part of strategies to generate distrust in journalism and delegitimize any information that is perceived as a threat, thus eliminating the counterweight that the press represents against the government.

3.3.1 Manipulating the presentation of information

Although bots are part of the structure of the Internet, their use to distort the content and the impact of information on social networks has begun to be problematized in the public and private context. In electoral processes around the world, bots have been used to simulate the popularity of certain content through "likes" and sharing, thus creating a context of polarization. This situation produces a false idea of popularity or consensus - as well as inaccurate information - about political ideologies and personal convictions. Companies like Facebook, Twitter and Google have shown concern about this and have started to create initiatives to eliminate bad bots from their platforms.

Behind the use of bots to manipulate the presentation of information is a whole political economy whose market is based on buying and selling botnets for this purpose. The offer of this service is not only found in the background of the dark web , but it is also available on the common and current Internet. Furthermore, with technological advancement, bots become more sophisticated and their detection and elimination by social media platforms becomes more difficult.

In this context, extremely effective disinformation campaigns have emerged that have involved sophisticated planning work. In the 2016 United States presidential elections, a series of false

stories were created with a dissemination strategy that included strategic data leaks and conspiracy theorizing, as well as the propagation and amplification of messages by means of bots until they arrive. to mainstream media . " Pizagate " is a good example of this. Hillary Clinton was the victim of a hack in her email, where they found receipts from a restaurant called Comet Pizza , which were used to affirm that the presidential candidate and her campaign advisor John Podesta carried out pedophile acts in the basement of said pizzeria. As a result, a person drove his vehicle to the pizzeria with a firearm, shot the sky multiple times during office hours and broke into the business looking for the alleged children who were trapped.

3.3.2 Trump

While fake news is not new to American democracy - let's recall the popular story in 2010 that Barack Obama was born in another country - these stories multiplied without similar precedent during the 2016 presidential elections. An Ohio State University study found that a significant number of Democratic Party voters were convinced not to vote for Hillary Clinton based on fake news . For example, some of those stories included that Clinton would be seriously ill and also that she had sold weapons to the Islamic State and other jihadist groups.

However, the case of Donald Trump posed challenges to the traditional approach of scholars of fake news . The strategy of the current president of the United States was, and continues to be, to use the rhetoric of " fake news " to disqualify serious journalism when it questions it or puts problems on the table that it does not want to address. In this way, since his presidential campaign, this character has waged a war against the media in his country, attacking the neutrality of information and arguing that they are the enemies of the citizens. Various authors have come to the conclusion that Trump uses this resource in the face of any news that he does not like, regardless of the accuracy of the facts that he narrates. This situation has generated skepticism about the information presented by the media and American journalism, both domestically and internationally.

3.3.3 Bolsonaro

During the 2018 presidential election campaign in Brazil, a series of fabricated news was reported against Fernando Haddad and the Workers Party (PT), the main adversary of current president Jair Bolsonaro. The members of Aos Fatos , a Brazilian fact checking platform made up of seven journalists in Sao Paulo and Rio de Janeiro, recorded a drastic increase in disinformation against Bolsonaro's adversaries, especially through WhatsApp , in two aspects: (i) the questioned, with conspiracy theories, the security of electronic voting and (ii) a constant relationship of the other candidates with minority guidelines, such as the LGBT agenda and the right to abortion. Some examples are the following: the “ gay kit ” that Haddad would have implemented in the Ministry of Education, the relationship between Bolsonaro's attacker and Lula, the interference of Venezuela in the elections, the legalization of pedophilia that would be implemented by Haddad, or the defense of incest that he would have made in one of his books.

A study carried out by the newspaper Folha de S. Paulo on 1,339 messages sent confirmed that 97 percent of the news shared by WhatsApp by Bolsonaro's followers were false or distorted.

In addition, the newspaper pointed out that a group of businessmen had invested at least 2.8 million euros to buy packages of massive WhatsApp messages with content denigrating the PT. According

to the Monitor of the Political Debate of the University of São Paulo (USP), Bolsonaro's followers were responsible for 38 million interactions, the contents of which are basically anti-feminist, anti-PT and hostile towards the traditional media.

3.3.4 Brexit

In the 2016 referendum held in the United Kingdom on its permanence in the European Union, Newsnight found a set of private groups on Facebook with millions of members where fake news circulated , especially focused on migration: for example, that the German authorities ordered sex workers have sex with migrants. An independent platform called Media Bias / Fact Check described one of these groups as "extremely biased, constant promotion of propaganda / conspiracies, poor or no credibility of the information, a complete lack of transparency." Likewise, the study of voter activity on Twitter concluded that pro-separation users had greater activity and prominence on social networks, which could have influenced the final result. However, it has also recently been reported that anti-Brexit groups paid hundreds of thousands of pounds to Facebook to spread fake news about Theresa May's implementation proposals in Parliament.

3.4 Social networks

3.4.1 Functioning of social networks

As of January 2019, around 3.484 billion people were actively using social media. This 45 percent penetration of virtual platforms has created the ideal environment - both for reasons intrinsic to their operation and for conjunctural reasons related to political and social crises - for fake news to spread quickly and powerfully. This technological phenomenon has not only affected the way in which people interact, but also their obtaining of information. Before its appearance, the news was published and circulated only by official media, such as radio, press or television, which had a filter, editing, verification and curation process. However, social networks and other virtual platforms have allowed the democratization of information and news, with the audience now being the creator and recipient of content.

The functioning of social networks per se is a clear facilitator of the generation of fake news . These digital platforms work based on algorithms, a type of artificial intelligence that involves logical encoded processes that help solve a problem, transforming input information into the expected response. In terms of social networks, algorithms are the basic operation, which allows the appearance and circulation of content, such as publications, suggestions, news, etc. But beyond the algorithms themselves - which are used in a series of fields and for different purposes - the conflict lies in the specific programming of each social network, which individually decides the way in which these processes will filter and organize the information. published information.

Facebook organizes and presents the information based on its level of significance. This is influenced by the publishing user - for example, it will be higher if it is a family member or close friend -, and the level of interaction they have - for example, more likes, comments or reactions. Thus, the information is published first to a small audience, and if it is received positively, it will migrate and expand its range of reach. Instagram adds two variables to this significance condition: time and category.

On the one hand, a post is more likely to be seen when more users or followers are online. On the other hand, the platform will first present the user with the content of the category with which they interact the most. This fact directly affects the creation of polarization and hyper-partisan groups: if a user tends to be interested in certain political opinions or news, the information that appears in their newsfeed will confirm their beliefs. The YouTube algorithm has been a promoter of the same. In order for users to spend as much time as possible watching online videos, the platform has tended to include conspiracy theories and misinformation in its "Recommended" section.

What began as a technological mechanism that promotes the consumption of social networks (the main objective of companies in the field), today affects the spread of fake news . On the one hand, it creates and exacerbates polarization - since personal interests will always be prioritized when publishing news - which implies a low level of diversity of media and points of view on the same news. On the other hand, it generates a dissemination of greater scope and frequency when a news item gets more likes or comments, which invites the creators of fake news to create even more extreme and striking content, only to gain greater significance. This hand in hand with the little analysis on the veracity of the content that allows an absolutely computerized mechanism.

Another aspect of the digital age that influences the spread of fake news is the ease of content creation by users, not only through the same social networks, but also with the development of professional-looking Web pages and many times identical to those of traditional media. On the one hand, there are web hosting or web hosting platforms , which provide web page creation services at no higher cost; on the other, sites like WordPress , Drupal , SnapPages or Joomla allow the user to create or personalize their websites. The accessibility, both physical and economic, of these platforms is an important component for the fake news created to have greater relevance and "credible" character. This reduction in monetary and non-monetary costs allows anyone to publish apparently true news without any filter. In addition to the amount of false information that is generated, the impact it has on the traditional media system must be questioned, which must meet standards and requirements for its management.

The contents themselves have to attract the attention of the users. That information, image or video that appeals to the emotions of these will have more natural success , since it will have multiple interactions.

However, this first contact by the close group will be amplified by the algorithms of each platform and will expand its reach, thanks to its relationship with emotions. While positive or pleasant content is more likely to be disseminated than negative content, those that generate arousal - positive or negative - are the ones that are disseminated more frequently. Therefore, fake news, which is usually intended to upset or generate conflict, fits perfectly as content that is likely to be published.

Finally, the economic factor also comes into play in the dissemination of this news. Like traditional media, social networks and websites depend on the revenue generated by the placement of advertising by third parties. Thus, benefit-based systems are created to attract a greater number of visits at the lowest cost. Likewise, the previously explained operation that favors publications with greater commitment or significance and the creation of fake news are combined to gain a profit. The spread is not dependent on the veracity, but on the likes, comments and reactions. Therefore, a bogus content generator takes advantage of this aspect to increase their income.

3.4.2 Technology for the generation of fake news

In addition to social networks, which form an idyllic context for the spread of false information but also have other harmless functions, the rise of fake news has been surrounded by the appearance of organizations and technological developments directly created for their generation.

The aforementioned fake websites, created for the sole purpose of generating fake news, are a prime example. ABCnews.com.co (United States), Retenews24 (Italy) and Nile Net Online (Egypt) are just a few pages that claim to publish information and truthful news, but whose hidden agenda is actually to influence their users and spread fake news .

Going deeper into the field of generating fake news and false interactions on the network, are the trol farms (or trol armies , armies of trolls). An individual who posts provocative messages on a social network or digital communication platform, with the intention of causing disruption and discussion, is considered a troll . The North Atlantic Treaty Organization adds the hybrid troll consideration , which communicates a particular ideology, and operates under the orders of an institution or state . Troll armies, then, are the set of these individuals under organizations, which systematically generate content. The means through which these individuals interact is the creation of fake accounts (multiple accounts for each one, for each platform) and the generation of publications, comments and broadcasts.

On the other hand, social networks and their users are currently endangered by the existence of bots, which fulfill the same function as trolls , but are actually computerized programs or software -

algorithms - programmed by organizations or users to auto-respond to predetermined comments and perform other functions preset by users. Bots have been studied to deceive nearly 30 percent of social media users.

3.4.3 The role of digital platforms

In addition to the visible impact that fake news has had on the elections of countries such as the United States or the United Kingdom, the dissemination of disinformation through social networks has also impacted emerging economies. 78 percent of the population of Tunisia, 76 percent of Lebanon and 72

percent of Vietnam claim to have seen fake news articles on these platforms. These figures suggest that the global impact of social networks in the field of fake news is important.

Furthermore, we must consider that social networks are nowadays the means of communication; however, they are not governed by their national standards and regulations.

A clear problem is its presence in several countries. Facebook has become a news outlet in 36 countries, with 54 percent of online users claiming to use the platform as a provider of information. Considering also the globalization of news and connectivity as a result of networks, this implies a difficulty for States to propose guidelines or regulations regarding digital content. On the other hand, social networks do not have the character of a means of communication, although they fulfill

the same functions. Therefore, they are not subject to the same conditions that the media must meet, such as data checking, editing, among others.

Unlike traditional media, social networks fulfill the role of information intermediaries. The contents are not generated by the companies, but by their users, so they do not have the ability to define what is expressed. However, the already discussed operation of the algorithms does influence the way of presentation, circulation and selection of usually false news at a mass level and with a greater scope, since it is based on the behaviors related to the publications, and not with the content.

There are two main positions regarding the role that should be taken to regulate the expansion of fake news in the digital sphere. On the one hand, the same technology companies regulating the speeches and news within their networks. For example, through a change in their presentation and suggestion algorithms (such as Google and Facebook), greater options to deport problematic content (Facebook) or the blocking and elimination of false or harmful users and content (Facebook). However, this can also have consequences: eliminations are not always made by individuals (so are algorithms) and even if they were, they suffer from their subjectivity to decide their negative or neutral category. In addition to this, it could be argued that these platforms do not have any legal obligation to censor speeches, which could give them more power.

The counterpart is in the efforts at the government level to develop regulations or guidelines for the operation of social networks in each country, and perhaps, at the international level. In Germany, the state is intervening with fines to companies that fail to remove illegal content reported by users. However, the laws that impose penalties on intermediary companies must be taken with care, as they can cross the line of freedom of communication. In addition, the State can generate even more marginalization and rejection on the part of the attacked groups.

3.4.4 Minorities and moral panic

The concept of moral panic refers to the social reaction based on the false or exaggerated perception of a group of people, usually a minority or in a vulnerable situation, as a threat to society. The information disseminated is generally exaggerated or fabricated by those who have been called "moral entrepreneurs", who create a threatening situation with inflated rhetoric and develop a sense of danger or fear towards a group of people. These speeches are channeled through the media and social networks, which allows those in power to dominate the information against those groups.

In recent years, some of the groups that have been subject to moral panic in Western political discourse have been migrants, Muslims, Afro and indigenous communities, and LGBTIQ people. However, each country has its own context based on the current situation. For example, in the United States, Latinx immigrants - especially Mexicans and Central Americans - are at the center of the discourse of moral panic legitimized from the White House and presented as criminally and socially dangerous. However, this representation in politics does not remain a mere narrative, but has consequences for the behavior of the US government: the idea of building a wall on the southern border, the elimination of benefits for undocumented students, increased police repression and the criminalization of Latino communities, hate crimes, among others.

The use of racial stereotypes, images, metaphors, emotions and the creation of “virtual lives” of immigrants are effective tactics used by moral entrepreneurs on digital platforms with the purpose of sending various negative messages against Latinx communities in the United States. .

In this sense, fake news appropriates threats made from moral panic to take advantage of them as political capital through a populist discourse. For this reason, conspiracy theories and false information use the social uncertainties present in a certain political and historical context to generate fear about the unknown or historically invisible: women's rights, sexual diversity, migrants, or indigenous or Afro communities. .

3.4.5 Intervention by other States

Following Donald Trump's victory in the 2016 US presidential election, a number of hints about possible Russian interference began to emerge. Investigations indicate that, under the personal will of President Putin, private and public Russian actors participated to aggressively influence US policy. While it cannot yet be stated with certainty, Putin could have successfully brought Trump to the presidency by attacking the Hillary Clinton campaign with the posting of emails on WikiLeaks and the anti-Clinton and pro-Trump news. shared by millions and produced by Russia. Specifically, the Russian strategy would have taken three paths: (i) the hack and dissemination of Democratic Party documents, (ii) a massive fraud on Facebook and Twitter, and (iii) contact with the Trump campaign.

According to the New York Times newspaper , about a hundred Russian trolls, hackers and agents participated in this intelligence work. First, officials from the Russian Foreign Ministry contacted Papadopoulos, Trump's campaign adviser, with the aim of showing interest in his election and the possibility of scheduling a meeting with Putin. As a result, there were a series of attempts by Russian agents to establish contact with the Trump campaign. These would have met in June 2016 at the Trump Tower in New York where they would have promised information harmful to his opponent, Hillary Clinton. Three days after this meeting, the alleged Russian promise came true: WikiLeaks founder Julian Assange went on television to note that a series of Clinton-related emails would soon be published.

Shortly thereafter, a hacker website named Guccifer 2.0 emerged claiming to have broken into the National Democratic Committee (CND) network and offering as evidence a series of stolen documents. It also pointed out that the rest of the documents had been handed over to WikiLeaks .

The day before, CND officials had warned that Russian hackers had managed to enter their network. However, both Russia and Assange denied these facts and have tried to link Guccifer with American and European citizens. In October 2016, the United States intelligence agency officially announced that the Russian government, with the approval of its highest officials, would be responsible for the hack and dissemination of CND emails.

On the other hand, Russian trolls would have been in charge of manipulating social networks to spread hatred by creating more than 470 groups on Facebook with hundreds of thousands of followers. These would have been created in the Internet Research Agency , the Russian company that would become the most famous manipulator of social networks in the world. For example, a group called Heart of Texas called for a protest against an Islamic center in Houston, even encouraging them to bring their firearms, claiming that the state of Texas was being "Islamized." Facebook acknowledged Russia's interference on its platform with an ad spend of more than $ 100,000. However, the scope of the Russian strategy was even broader: 2,700 fake Facebook accounts, 80,000 posts, and an eventual audience of 126 million Americans on Facebook alone.

Likewise, some experts have warned that Russian trolls would be spreading polarizing political messages to influence the 2020 presidential elections.

3.4.6 International right

Based on the experience of the United States in the 2016 elections, it has begun to discuss whether Russian interference may have violated any international norm. For this, it is necessary to analyze the following principles:

● Sovereignty : In recent years it has begun to question whether sovereignty - as a principle and as a norm of international law - applies to digital activities and infrastructures within the national territory, specifically in terms of cyberattacks. For example, the United Nations Group of 19 Government Experts on Development in the Field of Information and Telecommunications and the International Group of Experts that prepared the Tal inn Manual 2.0 on the International Law Applicable to Cyber Operations think so. For some authors, any operation that renders the digital infrastructure inoperable qualifies as a violation of national sovereignty that could, for example, prevent the voting system from producing valid results.

● Non-intervention : From the fundamental principle of sovereignty derives the customary rule of non-intervention in the internal matters of another State. For doctrine, this international obligation also applies in the context of cyber operations. For there to be an international illegal act, the operation must (i) affect the reserved domain of the State and (ii) be coercive.

If one of the two elements is not fulfilled, although it could constitute an interference, it would not be an illegal intervention.

● Due diligence : Due to the difficulties of proving a relationship between the State and private agents to attribute international responsibility to the former, the duty of due diligence can be used to maintain that the State should have taken the necessary measures to avoid said operation. This international obligation requires the State to guarantee that cyber-operations are not undertaken from its territory against another State.

● Self-determination : The right of self-determination implies the power to determine the future and the destiny of your political system.

● Privacy : Regarding International Human Rights Law (IHLR), the individual right to privacy could be violated, a situation that could give rise to an international claim in any of the international systems for the protection of human rights both at the universal as well as regional. This case would pose a challenge in terms of the extraterritorial application of international obligations in the IHLR.

3.4.7 Previous actions at the international level

A. Universal

The Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966)

Two of the main documents that outline human rights standards express the right of all people to express themselves freely, without any restriction on the grounds of race, gender, religion, among others. Likewise, this right focuses on receiving and seeking information, which must also be enjoyed by individuals. Despite the fact that the writing of these two documents was not focused on fake news - nor were these a problem at the time -, the stipulated rights are closely related to the production of fake news. This is a constant conflict for governments, since the regulation of fake news can confront the principle of freedom of expression.

Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda (2017)

The United Nations Special Rapporteur for Freedom of Opinion and Expression, the Representative for Freedom of the Media of the Organization for Security and Cooperation in Europe, the OAS Special Rapporteur for Freedom of Expression and the The Special Rapporteur on Freedom of Expression and Access to Information of the African Commission on Human and Peoples' Rights presented on March 7, 2017 in Vienna, Austria, this document that unites the perspectives and possible routes to face disinformation. The document identifies general principles and standards, as well as specific contexts where this is promoted and the different stakeholders involved. As for the principles, it delimits the possibility of restricting freedom of expression by the States, as well as the punishment received by both organizations and individuals. The standards focus on propaganda and misinformation by the state, as well as criminalization laws for defamation.

Journalism, 'False News' and Disinformation, A Manual for Journalism Education and Training (2018)

In 2018, UNESCO published this document, the creation of which responds to the importance of fake news in recent elections and political events around the world. Its objective is to be a model of a global curriculum so that member states can take it, adopt it or adapt it, and improve the quality of journalism in their territory. Different topics are touched on disinformation and the effect of fake news , also adding practical modules and suggested readings for journalists in training.

This manual is part of the Global Initiative for Excellence in Teaching Journalism, which focuses on promoting a global approach to journalism, as well as the exchange of good practices.

B. Regional

Internet Content Notification Unit - UE IRU (2015)

As part of the European Center against Terrorism, Europol creates this body to investigate negative content on the internet and social networks. This unit made up of 15 Europol officers focuses on the use of social media by terrorist groups, which, like many other organizations, use cyberspace to launch campaigns promoting violent acts. Until December 2017, the unit has been able to get 86 percent of the cases found to be eliminated.

European Commission High Level Expert Group on Fake News and Online Disinformation (2018)

This group was created with the objective of defining a strategy to address fake news at the European level, including 40 members from areas such as technology, civil society and journalism. The group has published a report in which they delineate the concept of fake news - which they deny giving such a term, preferring rather disinformation. On the other hand, the group has carried out surveys on the importance of quality communication media for the different countries of the European Union. Some of its recommendations focus on protecting the diversity of communication, educating citizens on media issues and other measures that the States and the Commission should take.

C. Private actors

In recent years, tech companies themselves have taken steps to limit the spread of fake news . WhatsApp introduced in 2018 a feature that labels forwarded messages, with the aim that the user can determine who generated the content sent. Facebook works with both its own and non-partisan fact checkers such as the International Fact Checking Network. In this way, it limits the publication of these news both by censoring them and by publishing them at the end of the news feed (home) of the social network. On the other hand, take action against organizations and individuals that constantly publish false news, restricting their publications and the scope of these.

Google is also introducing mechanisms to curb fake news . One of them is a tag that describes the articles that expose possible fake news , so that the platform can publish them at the beginning.

3.5 Possible positions by blocks

The way in which each country understands fake news and its consequences for democracy varies in each particular case. However, it is important to take into account a series of variables that will determine the position of each State in the current situation of the problem.

● Limits to freedom of expression : Some political and legal systems have been more reluctant to introduce restrictions on freedom of expression than others. For example, the American tradition, based on the First Amendment of the Constitution, has historically privileged the exercise of freedom of expression over the limitation of other rights. In contrast, European countries have usually more easily regulated the contours of freedom of expression in a democratic system where it coexists with other rights of equal importance. Asian and African countries have also been characterized by having more rigid limits on freedom of expression. This factor could determine the political will of each State to tackle fake news .

● Previous experiences: Democracies that have recently and publicly experienced the effects of fake news will have a particular vision on the subject. Countries such as Germany, Saudi Arabia, Australia, Austria, Belgium, Canada, Colombia, Czech Republic, Philippines, France, India, Indonesia, Israel, Myanmar, Poland, South Africa, Sweden and Ukraine have also had episodes of fake news in recent years . However, this does not necessarily mean that the consequences of misinformation have been understood or internalized by citizens and the political class.

● Government of the day: The ideology and particular interests of the political groups in power can influence the official position of the State on the issue, especially if they were benefited by fake news in their election as Trump in the United States and Bolsonaro in Brazil.

3.6 Possible solutions

● State regulation: As developed throughout the study guide, the option of some States has been to develop legal norms with the aim of proposing guidelines for digital platforms and sanctions for those responsible for the creation of fake news , both with financial fines as well as with measures of a criminal nature. However, in those countries that have chosen to establish restrictions on freedom of expression, recent history has shown that this decision has not been free of confrontation and political resistance at the domestic level, as in the case of France, which was previously exposed.

● Self-regulation: Another alternative presented in the study guide has been the possibility that the companies themselves implement mechanisms to identify and eliminate fake news from social networks. For example, a change in its presentation and suggestion algorithms, greater options to deport problematic content, or the blocking and removal of false or harmful users and content. Some of the platforms that have implemented some type of mechanism of this type are WhatsApp, Facebook and Google. However, these are still insufficient to stop their spread and the consequences they have on democracies.

● International cooperation: Regarding the prevention, investigation and punishment of possible interference by other States in internal democracies through fake news on digital platforms, solutions can be considered at a bilateral or multilateral level such as supervisory bodies, the elaboration of binding international instruments and the development of new technologies that help to this end through a joint effort. For example, through the signing of treaties, mandatory obligations could be established that include sanctions or specific effects in the event of non-compliance by any of the States parties. However, at present, the phenomenon of fake news has not yet managed to enter the field of International Law. These have been addressed in a very limited way by international organizations and have not been the subject of the most important conferences of political authorities in recent years.

3.7 Questions that every draft resolution must answer

A. Should International Human Rights Law regulate or evaluate the veracity of the communication media? up to what point?

B. How do the limits to freedom of expression operate in terms of hate speech and other forms of discrimination or violence?

C. How should the international community handle freedom of expression in digital media?

When is censorship configured?

D. How to ensure that the signifier " fake news " is not used in political discourse to delegitimize serious journalism?

E. How to guarantee the independence of the democratic system in the digital age?

F. How does fake news affect certain social groups in a different way?

G. What is the role of digital platforms in the regulation of fake news ? Are there still opportunities for self-regulation?