PEGASUS CASE: VIOLATIONS OF THE RIGHTS TO PRIVACY AND THE DEFENCE AND OTHER RIGHTS

SÍNDIC
EL DEFENSOR DE LES PERSONES

PEGASUS CASE: VIOLATIONS OF THE RIGHTS TO PRIVACY AND THE DEFENCE AND OTHER RIGHTS

SÍNDIC
EL DEFENSOR DE LES PERSONES

Catalan Ombudsman (Síndic de Greuges de Catalunya)

1st edition: June 2022
Pegasus case: violations of the rights to privacy and the defence and other rights. June 2022
Layout: Síndic de Greuges
Cover picture: (c) Pixabay

INDEX

INTRODUCTION

In mid-April 2022, *The New Yorker* echoed a report prepared by Citizen Lab, attached to the Munk School of Global Affairs and Public Policy at the University of Toronto (Canada). The report revealed that people in the pro-independence political and social environment had been spied on with malicious software (malware) such as Pegasus and Candiru, at least since 2015. The newspaper *The Guardian* had also echoed these reports in 2020 and Amnesty International had written a technical report about it in 2021.[1]

According to these publications, over 60 people from political positions, lawyers and people related to the Catalan independence movement were targeted by the Pegasus cyberespionage system, which was installed in their mobile devices. These technical results have been partially confirmed by the National Intelligence Centre (CNI), which admits to having investigated 18 people with this system, with the corresponding judicial authorisation. The Pegasus system was used in 13 of these cases.

Although Pegasus has been known to exist for years, there are some key factors that significantly heighten current concerns: firstly, Spain is the first case in which a European government has admitted to using this type of system; secondly, the targets of the investigation are high-level elected political officeholders, such as the former speaker of Parliament Roger Torrent and the current president of the Generalitat, Pere Aragonès; and thirdly, new case reports in Poland, Hungary, Germany and Belgium highlight the common use of cyberespionage tools within the European Union. The latest twist in the story has been the discovery that high-ranking Spanish government officials (Prime Minister Pedro Sánchez and Defence Minister Margarita Robles) have also been spied on with the Pegasus system.

The Catalan Ombudsman has the role of protecting and safeguarding the fundamental rights of the people of Catalonia when these rights are endangered by actions of the Public Administration. The Citizen Lab report reveals mass spying on Catalans linked to pro-independence movements or relatives of these individuals and their legal defence. Evidence also shows that this monitoring was carried out through the clandestine installation on their mobile phones of a hidden spyware program developed by the Israeli company NSO Group.

As a result of these events, certain institutional mechanisms were set in motion. On 4 May 2022, the Commission of Official Secrets of the Congress of Deputies was set up (after three years of legislation) and the person who was then the director of the CNI appeared in court. This appearance revealed that 18 Catalan individuals, all of them linked to separatist approaches and largely not subject to any criminal proceedings opened against them, were monitored by the CNI very particularly between December 2019 and the first quarter of 2020. According to the former CNI director, all the monitoring had judicial authorisation and followed the Intelligence Directive issued by the Spanish government in 2019.

It must be recalled that this directive is secret, as are the activities of the CNI, including petitions to the Supreme Court magistrate who must authorise interventions that affect the fundamental rights of people targeted for investigation, as well as how the investigations are conducted and resolved. The sessions of the Commission of Official Secrets of the Congress of Deputies are also secret.

In May 2020, the Catalan Ombudsman opened a first ex officio action on alleged spying on the speaker of Parliament at the time, Roger Torrent. The document was sent to the Catalan Cybersecurity Agency, which reported that its investigations into the possible compromise of the devices by Pegasus malware were not conclusive.

However, given the new information published and its scope, on 19 April 2022 the Catalan Ombudsman opened a new action that was moved to the Spanish Ombudsman, as the constitutional

[1] In addition to the report, the Appendix D and the Appendix E are also worth reviewing..

institution responsible for ensuring rights before all state administrations, including the CNI. The Spanish Ombudsman, which had access to all judicial authorisations relating to the espionage of the 18 aforementioned individuals, has concluded its investigation with a resolution dated 18 May 2022. Also of interest is the recent report by Amnesty International, *Pegasus: denuncias de vigilancia masiva en España* ("Pegasus: reports of mass surveillance in Spain").

Based on the Citizen Lab report, the references made to it by the media, the parliamentary interventions and court appearances of senior public officials of the central government and the report of the Spanish Ombudsman, the Catalan Ombudsman is in a position to present a brief institutional report on the scope of the impact of an intervention utilising malware such as Pegasus and Candiru on fundamental rights. The report is divided into two main parts: the first, which is technical in nature, sets out the technological characteristics and operation of these programs; the second focuses on how these programs can affect fundamental rights.[2]

[1] For the first part, the Catalan Ombudsman was helped by the company Evidentia, which specialises in computer expertise. For the second, it was assisted by Joan J. Queralt, Professor of Criminal Law at the University of Barcelona.

I. CYBERESPIONAGE: TECHNOLOGICAL CONSIDERATIONS FOR CITIZENS

1. TYPES OF CONTROL, MONITORING AND ESPIONAGE SYSTEMS

The goal of cyberespionage systems like Pegasus is to gain access to confidential and private information and communication conducted with computer devices. Of all the computer devices used by business and personal organisations, the one that contains the most sensitive information is the mobile phone.

Since the advent of smartphones, and given the huge popularity of iPhone (Apple) and Android-based phones, people have been using them to store huge amounts of personal information, such as photos, videos, documents, emails, electronic messages, Internet browsing histories, applications and more. These devices also have integrated video cameras and microphones, which can be turned on or off by applications and the terminal operating system, as well as geolocation systems based on GPS, WiFi networks, mobile phones and even Bluetooth.

The mobile is without a doubt the first object in history that knows almost everything about us, and we carry it with us wherever we go. This is why the information it contains is highly valued by companies, organisations and individuals.

It is important to understand that controlling or monitoring a mobile device is not always illegal or unauthorised. Everyone is being monitored in some way at all times. For example, the telephone network must know where the mobile device is at all times to direct calls to it and the law requires telephone operators to store and make this information available to state security forces and bodies to investigate serious criminal cases, though always with the corresponding judicial protection.

With the same motivation, the law also forces companies that provide digital services to keep the access data of their customers and users for one year. Therefore, email or website providers have to store information that could identify people who use their services.

On the job, the use of GPS geolocation is very well regulated to discover the position of workers when performing certain tasks, even using the geolocation services of corporate mobile devices. Under certain conditions, current case law allows companies to control computer tools, including email, to enforce corporate security policy. There have also been recent rulings that have legitimised the use of programs that take screenshots of staff computers, under certain conditions. However, this does not mean that all these computer products are legal in Spain.

The big difference between these commercial systems and systems like Pegasus is that commercial products typically require physical access to the mobile device or computer (or the local network used) and their access PIN or administrative password must be known. That is, it is very difficult for people to use them if they do not belong to one of the victim's tightest circles.

It is very important to understand that under normal conditions, it is very difficult for an average person to be spied on by a neighbour, acquaintance, ex-partner, co-worker and so on. In addition, the vast majority of computer and mobile phone operating systems incorporate measures to prevent them from installing or using programs that are hidden from the user.

It is very difficult to install and manage a spyware system on a remote computer or telephone without the owner's permission and so it operates in secret (or undetectably), as this requires cutting-edge knowledge of technology and very advanced technical resources. Therefore, these kinds of systems, like Pegasus, are only available to governments, security or intelligence agencies or security forces and bodies.

The conclusion of this section is that average citizens should not be afraid of being spied on by a cyberespionage system like Pegasus, and that they should be aware of the different types of monitoring that can be conducted from a mobile device and how (authorised and unauthorised). The uneasiness caused by Pegasus in the media must be leveraged to control the use of these powerful technological tools against elected political officials and the general public

2. TECHNOLOGICAL OPERATION OF SPYWARE PROGRAMS

All monitoring, control and espionage systems share a common technological basis and the difference lies in how each part is implemented. Below is a description of the common phases of the life cycle of a computer control technology solution, with details of the features of spyware systems like Pegasus.

2.1. Target location phase

This phase consists of knowing, for example, the telephone number of the person targeted by the computer control. The specific data depends on the attack vector, and in some cases it is important to know other data, such as email addresses, the type of device (including version) or other devices owned by the target person.

In corporate scenarios, with legal monitoring systems, this location is trivial and does not require any effort from the person who wants to install the software. However, in cases of cyberespionage, this location may not be trivial and may require tasks and sources of information only available to intelligence agencies or police forces. For example, the former president of the Generalitat Carles Puigdemont used a mobile phone without smartphone capabilities, which made installing Pegasus impossible. Faced with this obstacle, the attacker reportedly chose to infect and control people around him.

2.2. Infection or program installation phase

The nature of this phase depends largely on the type of case.

In corporate cases, company management delegates this task to the IT department, which has control of the entire computer park, usually corporate computers and mobile phones, so the installation effort required is trivial, as it is either done in person (the employee must bring the device to the computer department) or remotely.

Not all installations conducted by a company are legal or authorised. The legal nature of the use of these solutions in the workplace is not the subject of this report, but as a general consideration, the company must notify the staff of its powers of control and must use technological tools proportional to the intended objectives. Indiscriminate and hidden geolocation or screen controls are often considered illegal.

Without physical access, and without knowing access credentials, it is almost impossible to compromise a computer or phone with home media. In addition, manufacturers such as Apple and Google control the applications available in their web markets (App Store and Google Play) and do not allow spyware applications.

However, in cases of cyberespionage and systems like Pegasus, the story is very different. Companies like NSO Group in the computer security or cyber intelligence sectors have access to information about mobile devices that even their manufacturers do not know.

The Pegasus system is known to exploit security vulnerabilities that are unknown to mobile device manufacturers and therefore remain unresolved (known as *zero-day vulnerabilities*) to run computer programs that perform unallowed actions. In other words, they run programs that can dodge security measures in Apple and Android phones.

The investigations conducted by Citizen Lab and Amnesty International reveal that NSO Group exploited various unknown vulnerabilities in WhatsApp (Android systems) and iMessage, FaceTime and iTunes (Apple systems) to run unauthorised computer code.

There are three known methods of attack: in the first, the attacker sends a message to the victim, hoping to convince him or her to click on a link. Highly personalised messages are used to deceive the victim, such as notices from the Post Office to pick up a package,

from the Tax Agency, from the Business Registry or even links to alleged Twitter news.

According to this first method, when users click on the link, they are directed to a fake website that downloads a computer program to their mobile device, exploiting a security problem in some part of it to execute code without security limitations.

In the second method, the mobile device is intercepted by browsing the Internet, either by capturing traffic to the telephone system or via a device that emulates a telephone tower (and causes the mobile device to connect to it). When the victim enters an unencrypted Internet site (without SSL protocol), the attacker injects malicious code that exploits an unknown vulnerability to gain access to the phone, like in the first method.

The third method is the most effective and uses a security problem that can be exploited without user intervention. This method is known as *zero-click*. We know that between 2019 and 2021, Pegasus could be installed on certain Apple phones without any user intervention, exploiting vulnerabilities in iMessage and FaceTime applications: the attacker sent a notification to the phone with malicious content that allowed it to run code without security limitations.

When a phone is infected in one of these ways, the malicious code downloads and installs the Pegasus system, which is known as a *command-and-control system* (C&C), a computer program that secretly waits for orders from the attacker, such as to turn on the microphone or forward received SMS messages

2.3. Concealment and persistence

Cyberespionage systems like Pegasus can hide from the operating system and users. They usually try to leave minimal "footprints" for two reasons: firstly, to avoid getting discovered by users; and secondly, to evade discovery by security analysts and forensic computer experts.

Indeed, when a virus, Trojan horse or spyware system is discovered, a chain of events unfolds that usually ends the business of the spyware system manufacturer. First, the vulnerabilities that allow the initial infection and the installation of the C&C are discovered. Then, the manufacturer of the operating system or application is usually notified in private to give it time to resolve the issue and update all devices.

This is what happened with Pegasus. WhatsApp discovered the existence of 14,000 users of its system infected by a malicious program that was later identified as Pegasus, following investigations by Citizen Lab and Amnesty International. WhatsApp fixed the issue, notified the 14,000 users and filed a lawsuit against NSO Group, which was still open in the US District Court for the Northern District of California at the time that this report was drafted. This also happened with the vulnerabilities in iMessage, which were reported to Apple and resolved before being published.

Normally, the publication and solution of the vulnerability that allows the infection ends with the cyberespionage product. Yet the NSO Group has been finding new routes of infection (known as *new attack vectors*). In fact, several different attack vectors have been documented between 2015 and 2021.

Persistence is vital for spyware. It is the ability to remain in the infected device after it is restarted or turned off. Pegasus is not stored in the non-volatile memory of the phone, in order to minimise its footprint and its probability of detection. When the system restarts, Pegasus loses persistence, and a new infection is required. This inconvenience is not very important in mobile devices, as they are almost never turned off or restarted.

2.4. Sending of information

A key aspect of spyware systems is communication with the attacker: the attacker must execute commands and receive feedback from the infected system.

Currently, almost no computer remote control product allows direct connections between the controlling person and the controlled device. Instead, the connections are made by central servers that manage their interactions and operations. This makes it easier to avoid basic security measures such as firewalls,

because they are usually configured to filter data traffic from the Internet to the internal network, but do not usually filter connections from the internal network to the Internet. Many legal and common applications use this strategy.

Simple or legal remote control or monitoring applications typically use a network of easily identifiable proxy servers owned by the program manufacturer. In these cases, investigation of the data traffic generated by the control system can identify the type of software and its manufacturer, although it is generally not possible to identify the person or organisation controlling the device.

Instead, systems like Pegasus use a more complex strategy. In fact, they are believed to use a set of proxy servers for each Pegasus client. This ensures that a client cannot compromise or access another person's information on the same server.

It has also been found that NSO Group has taken action to make it difficult to identify its proxy servers. That is, the analysis of a mobile device can identify the proxy server with which it communicates, but it cannot establish that this proxy server is directly associated with NSO Group.

Both Citizen Lab and Amnesty International have managed to identify a good number of Pegasus control servers on the Internet. Their investigations have turned up Pegasus' "signature", meaning that they have determined a pattern of behaviour peculiar to Pegasus control servers. Once this signature was determined, other NSO Group control servers could be identified.

In fact, each time that Citizen Lab or Amnesty International have published details of what Pegasus' control servers are like, NSO Group has changed them and taken more and more action to try to hide them on the Internet. Up to four versions of Pegasus control servers have been found, each corresponding to one version and era of the system.

In the end, continuous monitoring of the traffic generated by devices suspected of having been infected with Pegasus can confirm their infection, both by the volume of data generated (if not justified by the applications and use of the system) and by the set of servers to which it sends them. In fact, the CNI used this method to confirm infections in the mobile phones of Prime Minister Pedro Sánchez and Defence Minister Margarita Robles.

2.5.Pegasus system capabilities

Little is known about the specific capabilities of the Pegasus system, but some feature lists have been published, including recording phone calls; reading SMS, iMessage and WhatsApp messages; reading emails; reading browsing histories; reading lists of installed applications; remotely activating the microphone and recording; and remotely activating the camera and retransmitting. It has not been found to spy on the secure messaging application Signal, which the Candiru spyware system, a competitor of Pegasus that has also been used against Catalan politicians, does support.

Pegasus can be installed on both iPhone and Android devices. Candiru can also be used against Microsoft Windows systems, extending the risk of infection to computers.

The most commonly mentioned functionalities of spyware systems are passive, in the sense that they are limited to taking existing information and data on the phone and sending them to the attacker through the proxy C&C servers. However, some of these systems also have "active features", with which the attacker can send emails and messages impersonating the victims. The main purpose of these features is supposed to be to activate accounts (for online banking, for example), but they could also be used to plant false evidence in devices that could incriminate the victims in actions or crimes they have not committed.

3. ESPIONAGE SYSTEM CONTROL

An important aspect of computer control systems is called auditing, which is merely the ability to know who has used the system, when and why.

In legal control systems, such as the computer control of equipment or corporate

tools, the IT department may install a control tool that can monitor staff activity data for some reason. For example, a geolocation data monitoring tool could be installed (for some legal and authorised reason) and, although IT staff may have access to the system to manage it, they should not have access to the data, as geolocation data are personal and can be very sensitive in some cases.

Modern computer systems allow this "separation of powers" and in practice allow the company's management to trust that the IT department cannot misuse it, and also to fulfil its duty of informing whomever (human resources, union representative, etc.) asks how and when the tool was used, what data it collects and who has accessed it. Modern computer tools can collect a record of activity that cannot be modified by the system owner, which can be used as proof of its use.

Audit functionality should be mandatory for computer systems that can affect fundamental rights such as the right to privacy or the right to secrecy of communications. Only with this functionality could we answer such questions as "Who was spied on?", "How long did the spying go on?" and "What information was monitored?"

Although many current computer systems, such as email, store certain activity information, these data are not directly available to users. For example, all email providers keep a list of the credentials of Internet connections that have accessed their email accounts. However, these data are neither public nor accessible to the individual account holder (some providers only provide data from the most recent days of activity). These providers only provide all data through a court order, which ensures proportionality and utility in the use of information that could be very sensitive.

In spyware systems like Pegasus, this traceability of the use of the system should be an essential functionality, but NSO Group has still not provided any information on Pegasus' activity in this regard in cases that have come to light. There is even conflicting information about whether NSO Group even really knows how and when its customers have used its system.

For instance, NSO Group is known to install a set of dedicated proxy servers for each client for security reasons. It is hard to believe that NSO does not monitor the status and usage of each client's system, for example, to add more servers should a customer's demand for service increase.

Moreover, cyberespionage companies are often subject to significant control by their government. We know that NSO Group must receive authorisation from the Israeli government to offer its products to new customers, which are limited to governments, intelligence agencies and security forces of countries with common interests.

This government control also occurs with other Israeli cyberespionage companies (Candiru, QuaDream, Paragon) and in other countries, such as Russia (with Positive Technologies) and China (with Computer Security Initiative Consultancy, a Singapore-based company that is believed to operate with Chinese technology).

Finally, there is an agreement between Israel and the United States not to use these spyware systems against US citizens. These conditions have been extended to the United Kingdom following the publication of news that government officials in that country may have been spied on with Pegasus as well.

These considerations make it difficult to believe that Israel will not impose a system of traceability of activity and audit on the Pegasus system and NSO Group, so it can know who is using it and against whom. It could also be possible that these data are secret, as is the very existence of the data.

On the other hand, the published data denote a certain lack of control by NSO Group in how its customers use the tool. Infections have been reported against politicians in European countries such as France, the United Kingdom and Spain, theoretically allied with the interests of the United States (and therefore Israel). The case of Spain is interesting, because it is also a client of Pegasus.

Certain publications could indicate that NSO Group provides a tool to its clients that reports whether a mobile phone is infected with Pegasus once it is installed. However, this tool does not seem to have been used in Spain, where Pegasus was apparently detected through data traffic analysis.

And yet Pegasus is clearly being used for a different purpose than those announced by NSO Group, which in theory are the fight against crime and terrorism. This purpose has also been publicly stated by other manufacturers of cyberespionage tools and, as far as is known, is also ignored.

Pegasus attracted the attention of groups such as Citizen Lab and Amnesty International precisely because of its use against journalists, politicians and human rights activists. There have been documented cases since 2015 in many different countries, such as Saudi Arabia, Morocco, the United Arab Emirates, Rwanda, France, Greece, Poland and Hungary.

In Spain, the CNI has admitted that it had authorisation to conduct cyberespionage on 18 people in the Catalan political sphere, but in reality, over 60 cases of spying have been documented. The reason for this difference remains unknown and it is doubtful that the lawsuits filed against NSO Group will end with an explanation by the company that could clarify the situation.

In short, the functionalities of audit and traceability of cyberespionage systems, protected by the judiciary, are essential to ensure minimum control of the use of these tools. This capacity for control should also be transparent, with obvious considerations of secrecy and confidentiality, which are also important in these cases.

4. ABILITY TO DETECT AND REPORT

What technical means do we have to detect spyware on our devices? In the specific case of Pegasus, we know that it is not stored in the phone's internal memory to minimise the likelihood of detection, but research by Citizen Lab and Amnesty International shows that, despite NSO Group's efforts, infection by and the execution of Pegasus leaves certain clues and traces that can be considered indicators of compromise that tell us if a device has been infected in the past.

Specifically, Amnesty International published its comprehensive analysis methodology and has been updating it with data obtained later. It has also published the list of the indicators of compromise that it has found for Pegasus and provides a free Mobile Verification Toolkit (MVT) to all Internet users to verify the presence of these indicators on their device.

The publication of the methodology is important, but it obviously gives NSO Group the opportunity to change its software in newer versions to prevent Pegasus from leaving these clues behind and making it more difficult to detect. In addition, computer tools have also come out that inject these indicators into a mobile phone, causing false positives.

Citizen Lab has only partially published its methodology and conducted a peer-review analysis of Amnesty International's methodology, meaning that it maintains some ability to track possible infections.

There are other methods of detection. For large and medium-sized companies, analysing the connections made to corporate phones and the volume of data sent can identify the presence of spyware systems not known to traditional antivirus systems. Companies and individuals can also always hire a forensic computer company.

II. IMPACTS ON FUNDAMENTAL RIGHTS

1. LEGAL PROVISION FOR INTELLIGENCE

The right to privacy and secrecy of communications is enshrined in Article 18 of the Spanish Constitution. Moreover, Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights recognise that no one may be subjected to arbitrary interference with their privacy, family, home or correspondence. Finally, Article 8 of the European Convention on Human Rights establishes the right to private and family life, in which only interference by public authorities established by law is acceptable, to achieve specific purposes (including public security and territorial integrity) that are necessary in a democratic society.

Thus, fundamental rights are not unlimited and may be affected in certain cases and under certain conditions, as long as their essential content is respected. These restrictions and the procedures for carrying them out must be accompanied by specific regulations in the form of an organic law, as established in the Constitution.

Such interference with fundamental rights may be of an individual nature and affect a subject or a small group of interrelated subjects, or it may be of a more general nature and affect the usual subjects of a territory. Among the first, we have the most common, which are those that result from a criminal investigation and, where appropriate, from convictions for crimes. Such provisions are found in procedural laws, from detention to the imprisonment of persons, including limitations on rights affecting privacy in its various aspects or property. Abusive implementation of these punishments, in principle legitimate, is also sanctioned by law, either by declaring the measures adopted null and void or by demanding personal responsibility from the person who adopted or executed them.

In this sense, the measures adopted by mandate or express authorisation of the Constitution can be of an investigative nature, such as criminal proceedings, in which facts are analysed because there are indications that a crime of a defensive or preventive nature has been committed, in the face of certain dangers established in the Constitution, such as the state of alarm of various intensities that has recently been experienced due to Covid, state of emergency or lockdown.

There are many measures that can be taken in defence of the state, understood in a broad sense and beyond the traditional and legal concepts of national security. In the face of certain indications, the law provides that a concrete and specific institution, which depends on the government and follows its annual guidelines, the CNI, may launch investigations of both isolated subjects and, more frequently, groups of citizens, Spanish or foreigners, which may affect the current constitutional system.

In order to perform these intelligence functions (i.e., an investigation to obtain information and interpretation of that information to make sense of it), in accordance with legal provisions, it may be necessary to conduct searches in closed places, such as homes or offices, and to check certain communications. The functions that the law rather vaguely entrusts to the CNI (Law 11/2002, Art. 4) entail needs for interference in rights covering personal, family, and professional privacy.

The constitutional coverage of these interventions is found in the generic statement of Article 18.3 of the Constitution, which submits them to judicial authorisation: “Secrecy of communications is guaranteed, particularly of post¬al, telegraphic and telephonic communications, except in the event of a court order to the contrary .”

Under the auspices of this authorisation, the law regulating the prior judicial control of the CNI provides that this body requests a “communications intervention” from a magistrate of the Supreme Court (Organic Law 2/2002, sole article). The law does not specify that this action must be motivated and, moreover, may be repeated without limit. The results of the investigations are not reported to the magistrate who authorised them, and neither the request nor the resolution must be made in writing. However, in no case can the results of this type of investigation be used in a criminal trial, since

they respond to different mechanics from that of the criminal trial, both materially and formally, meaning in terms of content and guarantees.

2. DIFFERENCES BETWEEN CRIMINAL INVESTIGATION AND INTELLIGENCE INVESTIGATION

A criminal investigation is launched because there are reasonable indications that a crime has been committed. In contrast, intelligence research is conducted to observe what is happening in areas that are not easily accessible, rather clandestine, or at least far removed from public scrutiny and observation, but sensitive to the functional goals of the CNI, without these cases having to be even indicatively criminal. Therefore, unlike criminal investigations, intelligence investigations constitute prospective investigations, which are constitutionally prohibited in criminal investigations, and are therefore more prone to invading spheres of privacy in a way that is not always legitimate.

The good that is protected in a criminal investigation is that which fits the object of protection of each legal definition of a crime, meaning life, freedom, sexual integrity, privacy and so on. However, the objectives that define intelligence activities are not strictly defined in the Constitution and those that are defined have a degree of indeterminacy that allows a very wide range of action, with easy danger of overflow.

At this point, it is worth comparing the requirements to be followed by court orders affecting fundamental rights in criminal proceedings or in intelligence actions. The criminal process in investigations that affect people's rights to privacy is strictly regulated, especially since 2015. As a general rule, non-compliance with legal requirements at least involves nullification of the evidence that may have been obtained through such defective interference. However, there is no legal provision for expelling intelligence actions from the legal system that do not even meet the minimum requirements provided by the law of the sector.

In fact, focusing on the topic that motivates this report, dubbed *Catalan-Gate*, since the content of any request for authorisation by the CNI has not been revealed, in principle there is no possibility of assessing whether the administrative request has met, albeit approximately, the criteria that must cover both the police requests in the criminal investigation headquarters and the judicial interlocutory decrees authorising them. This doctrine and its legal basis could give some weight to the simple regulation provided for by government intelligence action, in terms of both formulating the request for judicial authorisation and granting the authorisation.

After analysing the interlocutory decrees of the Supreme Court that authorised the interventions in the mobile devices of the 18 people subject to supervision in the Catalan-Gate case, the Spanish Ombudsman found "a high level of detail in the information available to the magistrate of the Supreme Court to be able to take a decision of authorisation or non-authorisation" and said that the interlocutory decrees "were extensively motivated, essentially based on specific facts".

However, taking into account the rights of the request for authorisation by the intelligence services, and in view of the information made public by Citizen Lab, which nobody has contradicted, the Catalan Ombudsman at least raises a series of questions about the possible fundamental rights affected and concludes with some recommendations derived from the doctrine of the highest body protecting fundamental rights in Europe: the European Court of Human Rights (ECHR).

With the data available today, and given the legal secrecy that shelters the actions taken (both the 18 that have been publicly recognised and the others), it can be concluded that any interference with the fundamental rights provided by the Constitution rests on two essential pillars. One is necessity and the other is proportionality. The presupposition of the two pillars is the principle of legality.

These elements are discussed below in relation to the rights that presumably have

been or may have been affected by the aforementioned interference.

3. GUIDING PRINCIPLES OF INTERFERENCE IN FUNDAMENTAL RIGHTS (I): THE PRINCIPLE OF LEGALITY

We start with the common ground of all the effects caused by the public authorities that aim to be justified in the sphere of citizen rights. The condition or requirement of legality operates in two ways. The first is obvious: the measure to be practiced in the field of basic rights must be specifically provided for by law; in this case, the law must be the Constitution itself, developed by organic law. With regard to what is of interest here, the law provides that judicial authorisation is required to access the communications of the subjects to be monitored.

3.1. The principle of legality: scope of interference

As seen in the first part of this report, since the interference carried out by Pegasus technology provides full access to mobile phones, it should be stressed that is illegal to access the information and data contained in the infected mobile phone. Indeed, according to the Constitution, it is only lawful to access communications, meaning interpersonal contacts, through the system of physical or virtual networks available. However, it is not legal to access the rest of the information that such a device may contain, which is a lot.

This extreme is vital when we consider that smartphones are much more than conventional phones. They are in fact miniaturised, multifunctional computers, with a myriad of data that have nothing to do with interpersonal communications. For example, the daily calendar, contacts, documents, graphic and sound files and images in any format (even all kinds of films), scanned data, QR codes and family photos contained in smartphones are not forms of communication, but objects that belong to the person who owns the phone, regardless of how the photos, data or other documents have been inserted into the device.

Moreover, access to documents or other types of files that are in the cloud and can be downloaded to phones does not actually constitute communication, since no interpersonal communication is established. Indeed, the communication does not take place with any person other than the owner, but consists of remotely accessing a file that can be downloaded in whole or in part, or even simply viewable, without contacting anyone else.

Interestingly, unlike in a legitimately authorised criminal investigation, the tracking of people by telephone falls outside the legal concept of communication, since the ambulation, transfer or transport of a person physically does not involve any personal intercommunication. Tracking a beacon installed on a cell phone is not communication between two subjects, one of whom is the subject of the investigation.

Thus, with reference to Spanish law and without the need to verify the content of any petition or judicial authorisation, we can legitimately say that in no case can you legally access a telephone in an intelligence investigation to obtain information other than interpersonal communications.

3.2. The principle of legality: reasons for interference

A second aspect of legality related to the field of intelligence has to do with the motives or reasons affecting the integrity of what is called the *institutional system in force*. It is certainly a vague concept and one that is difficult to define. However, directing intelligence actions to interpersonal communications has nothing to do with the integrity of the institutional system in situations that affect several or many other various fundamental rights of privacy, or with goals foreign to this basic institutionalisation, such as political, personal or commercial interests.

In this way, the actions are stripped of legal coverage and the principle of legality is violated in this aspect when communications and more integral elements of people's privacy are observed that affect other fundamental rights, such as the right of

defence or negotiations between parties after elections to form a government

a) The right of defence

Indeed, the right of defence not only covers the defence of the claims of the persons concerned before the courts and other public authorities, but is based on the confidentiality presiding without exception over relations between lawyer and client. In the most extreme case, that of charges for the most serious crimes, in which, therefore, there is already a procedural case, the right to defence and the freedom of communication between lawyer and client in any place and under any circumstances is inalienable.

There are rights such as personal freedom or the secrecy of communications that can be suspended individually or collectively. This is not the case with the confidentiality between lawyer and client, which, as we say, is the basis of the right of defence, which, in turn, is one of the manifestations of the right to a public trial with all guarantees. This right may not be restricted under any circumstances. Indeed, violating this right has led to some serious criminal punishment, even against some judges, and has disqualified those responsible from holding public office.

In the context of prospective judicial authorisations, a critical situation may arise that could in fact render inoperative the right to defence and confidentiality between lawyer and client. Since the magistrates who can give these authorisations belong to two chambers in which some of the people being investigated face pending lawsuits (meaning the administrative and criminal chambers, both of the Supreme Court), by authorising the observation of the communications of these people, these magistrates could secretly come into contact with their procedural strategies. This would lead to an irreparable injury to the right of defence.

As indicated below, since these magistrates are not appointed according to a public and objective system, but according to a system aimed at the election of a judge determined for reasons not stated in the law, the shadow of doubt about the right of defence grows even greater and comes closer to the line of a constitutionally unacceptable risk.

b) The right to political participation

Moreover, the right to participate in public affairs is also not subject to legitimate intervention, regardless of the context. Access to communications and other contacts, intercepting documents or observing negotiations, whether formal or mere contacts between political parties, is radically contrary to current legislation. The confidentiality that presides over these negotiations is as the parties wish, so it is only up to the parties to the negotiating process to reveal to the public what they agree or the general state of the negotiations. Infringing this right is even more serious, as the rights of the represented and their representatives are violated. Indeed, these are negotiations between political forces on which there is no presumption of illegality, regardless of the purposes they pursue, since the Spanish Constitution is not a militant constitution, unlike others. The right to participate in public affairs has, in this case, been compromised.

3.3. The principle of legality: the judge predetermined by law

The judge designated to authorise interference in people's communications is appointed ad hoc, without competition, by the Plenary of the General Council of the Judiciary (Art. 127.4 of Spanish Organic Law 6/1985, of 1 July, on the judiciary).

The Constitution establishes that judges be determined by law, in general and not for a specific matter, as a basic fundamental right guaranteeing objective judicial impartiality and legal certainty for each person. With this personal appointment of a judge for a specific and extremely delicate case, there is a risk, because the judge assignation will not be automatic, as in other court cases. Instead, a particular judge will be appointed for a specific and unique type of case with specific characteristics. In this case, it is not the law but these personal characteristics that would establish the competition. This form of personal appointment may violate the character of a general provision for the assignment of powers, as provided for in the current legislation for knowledge of jurisdictional matters.

Current regulations, to some extent of dubious constitutionality, seem rather ideal for appointing a magistrate who is a priori more favourable to the pretensions of the CNI than to safeguarding the people's rights.

4. GUIDING PRINCIPLES OF INTERFERENCE WITH FUNDAMENTAL RIGHTS (II): THE PRINCIPLE OF NECESSITY

As for necessity, as both ordinary and constitutional jurisprudence has pointed out, an infringement on fundamental rights must really be the last resort, meaning there must be no other measure that can be put into practice that meets the objectives proposed by the investigators. In the same way, as jurisprudence also points out, the convenience of the body or the ease in the execution of the measure cannot be confused with the need for it.

The need for interference is really the competent public authorities' last resort. In other words, if there are ways that are more difficult but less invasive, they should be used. Therefore, use of these invasive measures of fundamental rights is only constitutionally legitimate to the extent that no other course of action is feasible.

However, there is currently no external and accessible element that allows us to assess this extreme when formulating requests and when issuing the court ruling authorising them, even when shaping the practice to the requirement of necessity.

In addition, this requirement is imposed by the authorisation of the intervention and, where applicable, by the authorisation of the extension. That said, there is no legal provision regarding the judicial weighting of the final result. This means that, ultimately, the need for interference in communications may become a merely pro forma assessment, never materially verified by an independent authority.

Finally, it bears repeating that from the point of view of legal provision, only the observation of communications can be massive and not that of other objects that can be obtained because they are on the mobile device or on any other type of device that allows interpersonal communications, whether the scope of the observation covers a subject or a group of subjects.

5. GUIDING PRINCIPLES OF INTERFERENCE IN FUNDAMENTAL RIGHTS (III): THE MANDATE OF PROPORTIONALITY

Proportionality or, in negative terms, the prohibition of excess, plays a preponderant role in the field of interference in fundamental rights. When intercepting communications conducted from a mobile phone, such as today's smartphones, or from other devices, such as desktops, laptops and all kinds of tablets that are connected on the telecommunications network, objects other than the communications themselves cannot be accessed. It must be remembered that all other materials contained in it are constitutionally and legally excluded, no matter how much interest there may be in obtaining and analysing them. Thus, the proportionality mandate requires the

immediate destruction of the data obtained in an observable device, without any further contact than this destruction.

That said, and following the guidelines developed by the Venice Commission in 2015[3] in relation to intelligence observations and a set of decisions by the ECHR,[4] a solid doctrine has been set up in which necessity and proportionality are the basis of intelligence functions on communications and other aspects of privacy.

It is no longer just a matter of the classical conception of proportionality as a judgment of whether the benefits of interference with fundamental rights must outweigh the possible violation of rights. It is now also a question of whether these judgments of necessity and proportionality must be verified at a later date, at least once the observation has been made and there has been an assessment of the extent to which the rights to privacy and other rights fundamental rights have been affected within the constitutional parameters.

This verification must take at least three key factors into account. First of all, the verification of the interference process must be carried out by an independent body, other than the body that carries out the intelligence investigation, which may or may not be judicial. Secondly, the results obtained by interfering with the violated fundamental rights must also be independently verified. Lastly, the affected people should be given the opportunity to verify the impact and to be able to go to court, if necessary, if they find that their constitutional rights have been violated.

None of the aforementioned bodies, neither the Venice Commission nor the ECHR, deny the need for intelligence investigations, even massive ones, in the various most sensitive areas of today's society. These interferences, however, must be carried out with the guarantees essential to a democratic society. After all, control of the legitimacy of the interference can only be carried out later by both an independent body and the person concerned. This is what the ECHR calls *end-to-end safeguards* in its resolutions, meaning being able to subject interference with fundamental rights to control from beginning to end, so that the process of interference fulfils all the guarantees. In fact, this is what happens in procedures or in complex digital applications in which the procedures are verified automatically, without the need to add any more elements.

The effective enjoyment of these guarantees is only possible if the persons affected are aware, at a given time, of the interference to which they have been subjected. For this reason, the May 2022 Amnesty International report not only states that judicial oversight is essential, but that those affected should be informed, wherever possible, that they have been subject to surveillance or that their data has been compromised.

[3] Venice Commission. *Report on the Democratic Oversight of Signals Intelligence Agencies*, adopted at the 102nd plenary session (Venice, 20-21 March 2015). Study no. 719/2013, Strasbourg, 15 December 2015.
[4] See the judgments of the Grand Chamber of the ECHR of 4 December 2015 (Roman Zakharov vs. Russia) and 25 May 2021 (Big Brother Watch vs. the United Kingdom and Centrum för Rättvisa vs. Sweden).

III. CONCLUSIONS

Global cyberespionage systems are a reality in Europe and will spark discussion and reflection on how intelligence agencies and security forces should control the use of these technological resources.

Governments and intelligence agencies will surely need these services, whether they are their own, as in countries with technological resources such as the United States, Russia and China, or hired, as in most European countries. They will also have to learn to defend themselves and avoid situations such as those caused by Pegasus in Spain, the United Kingdom, France and Greece.

From the information available, it can be presumed that the use of these systems on 18 private citizens has respected formal legality, but at the same time there is no doubt that it may have been an attack on fundamental rights, including the right to privacy and, in some cases, the right to defence and political participation. As for the over 40 other people allegedly spied on with Pegasus, everything suggests that no legality has been respected and that the interference with their fundamental rights has been without restrictions and without any control.

For this reason, from the point of view of safeguarding human rights and fundamental freedoms, the Catalan Ombudsman considers that:

1. According to the examination required by the actions recognised by the CNI and those documented by Citizen Lab and Amnesty International, which have not been contradicted, it can be presumed that there have been unjustified violations of the rights of the people observed, in other aspects of their personal, family and professional privacy, in their right of defence, in their right to confidentiality between client and lawyer, in their right to participate in the management of public affairs by themselves or through their representatives and in their right to a judge predetermined by law. A reparation by the public authorities involved would therefore be required.

2. Intervention in "communications", constitutionally and legally provided as a limit on the right to privacy, does not in any case protect access to all the information that smartphone-type mobile devices may have, even with judicial authorisation.

3. There is an urgent need to reform the Spanish Law of Official Secrets, which is in line with the rules issued by the Venice Commission and the ECHR. In this sense, it is necessary to establish a public and collegiate system of judicial authorisation and control with respect to the observations of the communications that the intelligence service requests within the framework of the law. Indeed, we must move from a single-judge system to a collegiate court and its members must be appointed publicly in any case, through the corresponding competition between the magistrates of the Supreme Court, if deemed appropriate. The appointment of the magistrate in charge of authorisations and controls may not depend on the appointment of the President of the General Council of the Judiciary alone, ratified pro forma by the Plenary Council.

4. It is also necessary to set a time limit on the observations of the communications, since with the current legal design they could be indefinite, without the observed subjects having committed any violation of the law or knowing that they are being monitored.

5. Once the governmental observation has been completed and concluded with an evaluative judicial resolution, it should be transferred to the people concerned, reservedly, but with full access to the administrative and judicial file produced, so that they may allege what they consider appropriate regarding the possible violation of their rights. In this way, they would receive a legally founded and appealable resolution, if necessary, to safeguard their constitutional guarantees.

6. The law must explicitly state that the observations of members of political parties, trade unions and associations of any kind that are legal, meaning constituted in accordance with the law and without being sanctioned, including legally dissolved or even banned, are excluded from the investigation.

7. The letter of the law must also state the prohibition on observing relations between a client and his or her lawyer or of interfering with them in any way. These relationships may not be observed or recorded in any event or under any circumstances. In the latter two cases, the legal reform should make special reference to criminal liability if the aforementioned anomalies occur. From this point of view, the Catalan Ombudsman recommends that the professional legal associations of Catalonia (and the council of associations in particular) promote actions to guarantee the right of defence in cases where the relations between client and lawyer have been affected by illegal wiretapping.

8. Manufacturers of cyber intelligence systems should be subject to audit controls and be required to identify customers and victims under certain conditions consistent with the secrecy required by their business. Technologically speaking, this traceability is possible and is compatible with respect for the confidentiality of the people involved. The functionalities of auditing and traceability of cyberespionage systems, supervised by the judiciary, are essential to ensure minimum control of the use of these tools. This capacity for control should be transparent, with obvious considerations of secrecy and confidentiality, which are also important in these cases.

SÍNDIC

EL DEFENSOR DE LES PERSONES

Síndic de Greuges de Catalunya
Passeig Lluís Companys, 7
08003 Barcelona
Tel 933 018 075 Fax 933 013 187
sindic@sindic.cat
www.sindic.cat