cap
cit

Consell Assessor
del Parlament sobre
Ciència i Tecnologia

Cyber security and privacy report for the Parliament of Catalonia

Executive summary

This document responds to a request from the Parliamentary Advisory Council on Science and Technology (CAPCIT) with the aim of making a report on cyber security and privacy for the Parliament of Catalonia. This report does not intend to provide exhaustive or rigorous information from an analytical point of view of the different types of attacks and mechanisms to protect us, but rather it tries to offer an overview that does not require specific training in the field of IT engineering.

The document is structured in two large sections: the first corresponding to cyber security and the second addressed to privacy. Subsequently, a best practice guide and conclusions are included.

The cyber security section classifies the most common types of attacks (social engineering, application vulnerabilities, APTs, ransomware), indicating their features, impact and mechanisms for mitigating these attacks. At the request of the petitioner, information on the Pegasus attack has also been added.

The privacy section begins by classifying data according to its sensitivity, and introduces the technologies used to protect privacy in a simple way. Subsequently, an indication has been given as to which of these technologies are to be used in the different stages of the information life cycle. Finally, the report indicates which laws allow us to regulate privacy in our environment.

Introduction

Cyber security is the protection of systems, networks and digital data against computer attacks. It is a critical and indispensable discipline that protects our data, privacy and society as a whole. Cyber security attacks can be carried out by a wide range of actors, including ethical hackers, cybercriminals, state hacker groups and others. Thus, cyber security becomes a vital necessity for companies, governments and individuals.

Today's society depends increasingly on ICT and this forces us to put more focus on resilience. While traditional cyber security focuses on protecting information, cyber resilience, understood as the ability to prepare, respond and recover from a cyberattack, will be fundamental to limit the impact of cyberattacks and guarantee the continuity of essential services.

Cyber security is a shared responsibility: both individuals and organisations must take steps to protect themselves from cyberattacks. Global spending on cyber security during 2022 exceeded 260,000 million euros and is expected to grow by 15% annually until 2025. The increase in cyber security budgets is a consequence of the relevance that this field is achieving in the development of digital society.

A cyberattack is an action or series of actions taken by an attacker with the aim of compromising or damaging a computer system, network, device or the data stored on it. There are several types of classifications of cyberattacks depending on the objective, methodology or their impact. Depending on the objective, these attacks can have various purposes, such as unauthorised access, theft of information, sabotage or destruction of data, denial of service, among others. Unfortunately, no system is immune to attack. Any entity that manages, transmits, stores or otherwise processes data must institute and enforce mechanisms to monitor its IT environment, identify vulnerabilities and close security holes as soon as possible. However, institutions are not the only ones that need to take measures to ensure cyber security. At the individual level, a series of actions can also be taken to protect data and devices, such as using strong and unique passwords, keeping software up to date, avoiding clicking on links or opening unknown source folders, using a trusted antivirus programme and being aware of cyber security risks.

A complementary discipline to cyber security and intimately linked is privacy. Privacy is a person's right to control information about themselves. This right includes the right to decide who has access to personal information, how it is used and whether it is shared. Privacy is a fundamental right that protects the freedom, security and dignity of people in an increasingly digital and connected world. Maintaining the balance between using data for legitimate purposes and protecting privacy is a major challenge in today's society.

Privacy is important for a number of reasons. Firstly, it allows individuals to protect their personal intimacy. Secondly, it promotes freedom of expression. Thirdly, it protects basic human rights, such as the right to freedom of opinion and the right to protection against discrimination. Privacy can be threatened by the collection and sharing of data between entities, the sale of personal data to third parties, and computer attacks that can steal personal data.

There are several privacy laws and regulations that protect individuals' privacy rights, setting requirements for entities on how they can collect, use and share personal data.

Most common types of attacks

Nowadays, attacks are very diverse and increasingly complex because as protection systems improve, attackers are becoming more professional and devote enormous amounts of time to training and taking advantage of the slightest error to be able to carry out their cybercriminal acts. Many of these attackers have become professionalised to the point of creating structures and management systems typical of military or business regimes.[1] So, we are facing a new era, where organised cybercrime must be taken very seriously.

Despite the progress made in cybercrime, in general, repeatable patterns can be observed in attacks, so that in practice, given the great diversity that exists, relatively similar attacks can be found.

Thus, even today, the most common types of attacks are based on social engineering and security errors in the applications used. That is why this chapter focuses on the description of social engineering attacks, to continue with a detailed explanation of attacks caused by software vulnerabilities, then passing the discussion on two derivatives of these more basic attacks, attacks with ransomware and Pegasus, which remain a combination of the previous ones.

Social engineering

Although at first glance it may seem that social engineering is not an attack, the effects it can have make it necessary to rethink this premise. Social engineering manages to violate privacy, one of the first pillars of cyber security, and it does so through one of the most important points when talking about cyber secure environments, the collection of information from the victim.

So, what is social engineering? This is an attack in which the victim is deceived through psychological tricks in order to, through a false sense of urgency, reveal sensitive information or force the victim to compensate the attacker financially.

Social engineering is considered one of the most common attack vectors today; so much so that social engineering is considered the most used attack during 2022, especially with one of the most common forms, *phishing*, which is estimated to account for 33% of all attacks carried out. Social engineering is rarely the end of an attack, but rather the means to subsequently obtain a return on the information obtained.

In general, an attacker will look for someone's personal information in order to:

[1] https://www.kelacyber.com/wp-content/uploads/2022/03/KELA-Intelligence-Report-ContiLeaks-1.pdf

— **Impersonate** the victim in order to profit financially or to be able to use it as leverage to obtain more information from someone else.

— Getting the victim to carry out some **action**, such as a bank transfer or granting permission to allow the attacker to carry out some operation, which is usually monetary.

Features and impact

There are many types and variants of social engineering, depending on the mechanism used to gain the trust of the victim and thus succeed in carrying out the attack. The most typical mechanisms are:

— **Phishing**: where the attacker sends a message pretending to be someone they know. The acquaintance can be someone from our contact book, but it can also be some service provider. In this category, they are known[2] messages pretending to be a bank, a delivery company or a post office.

There are several types of phishing, and they are becoming increasingly more well-developed. Spear Phishing is the most dangerous, where the attacker first carries out an exhaustive analysis of the victim or their organisation, and then creates a personalised message, even impersonating someone known to the victim, which is much more credible than a generic email from an external entity. There are well-known examples of this type of attack, such as the one suffered by Barcelona City Council, where, through the impersonation of a supplier, it was possible to change the account number of their payments to one controlled by an attacker, managing to divert over 350,000 euros.

— **Whaling**: is a variant of phishing which is very common where the target is company managers or political leaders. In this case, the attacker pretends to be another high-ranking executive or politician from another entity via e-mail. The message usually contains some false emergency or a great opportunity that will last for a short time and requires quick action by the victim. Generally, the goal is to obtain sensitive information.

— **Honey Trap**: this variant typically uses well-known social networks, such as Instagram, WhatsApp or Telegram. The goal is to send a message impersonating someone who wants to maintain a romantic relationship, and, once trust is gained, ask for some kind of immediate help through an invented problem, asking for urgency in order not to give time to think about the truth of the message.

— **Baiting**: the objective in this case is to obtain sensitive information from the victim, which is why it is sought that the victim fill out a questionnaire or document with this information or redirect it to a fake Google or Microsoft login page to steal their credentials.

— **Pretexting**: the attacker creates a fictitious scenario, for example pretending to be from the technical service of some company and saying that to fix a problem, also fictitious, in which the victim must provide personal data, such as credit cards or passwords, to continue using a service.

The impact of this type of attack is difficult to quantify, mainly because many of the victims, either out of shame or lack of information, do not report the act. However, as can be seen in the *Internet Crime Complaint Center (IC$_3$),* over 300,000 attacks are estimated to have taken place in 2022.

In addition to this, a critical aspect of social engineering attacks is that it is one of the most common *attack vectors* used by organised cyber-crime groups to gain initial access to a system. Once inside, it looks to spread throughout the network before launching a coordinated attack against the victim. An example of this is the attack suffered by the Autonomous University of Barcelona, where the attackers initially used phishing to obtain an employee's credentials to later carry out a ransomware attack.

How to mitigate social engineering attacks

There are several ways to mitigate, or at least minimise the impact of this type of attack, but this always involves two fundamental pillars. On the one hand, it is necessary to have the necessary technological tools, usually security monitoring applications of our systems, but also, and equally important, making employees and users of our systems aware of how to act and how to detect this type of fraud. This awareness usually involves providing employees with cyber security courses with practical cases to be able to observe first-hand how this type of attack works.

This awareness usually goes through the verification of a list of points to consider before publishing any type of information on the network. The most important are:

— **Determine** if the mail received is from the person who claims to be. That is why it is recommended to observe in detail the domain from which the mail was

[2] Campañas de suplantación de entidades bancarias con falsos cargos y bloqueo de cuentas

sent. That is, from the "@" of the mail to the end: there it is necessary to see exactly the expected domain, without any errors or letters different from what it should be (user@microsoft.com is not the same as user@micosoft.com).

- Be suspicious of any conversation, especially if the sender of the message is unknown.
- **Avoid** downloading email attachments when they come from unknown sources and contain applications. To know if an attachment is an application, it is necessary to see the file type. Applications are: EXE, MSI and even VBA files.
- **Make sure** that the links in the e-mails are correct. This must be observed by hovering the mouse over the link and see which domain the link will lead to: check that the domain leads to where it should go. To do this, it is necessary to observe the entire content of the URL, especially from "https://" to the first "/" of the name; so the domain of the URL https://www.gencat.cat.in/noticies/2023-07-22/ does not go to the website of the Generalitat. It is therefore recommended that, instead of clicking on the links, the website is accessed by typing the page to be visited directly into the browser.
- **Verify** the identity of the interlocutor through alternative methods, such as a phone call or validating the address book.

Controlled phishing attack campaigns are needed from time to time in order to get an idea of the awareness of employees or ICT users, so that employees learn to detect them and act accordingly, above all by creating a climate in which it is possible to report freely if such an attack has taken place, without reprisals for the possible victim, who may hide the fact out of shame or disciplinary consequences.

Attacks caused by vulnerabilities in applications

Given the large number of devices that are currently connected to the Internet, the large amount of software they have, and the huge number of users, it is normal that this software may contain errors. These errors may be functional, where the application does not act as expected, but others may simply be programming or configuration errors that are not perceptible to users, but can be exploited by a malicious attacker to force the application to behave in an unexpected way, thus causing potential extraction of information or allowing the attacker to take control of the affected resources.

This second group of errors is known as vulnerabilities and are a huge source of attacks, especially with non-updated applications or non-validated applications that may contain many of these errors.

Features

While social engineering attacks involve an action by one or more users, application vulnerabilities, in contrast, manifest themselves through failures in an application that allow an attacker to perform malicious actions on the victim's computer, be it a mobile, a desktop computer or the server hosted in a data centre. This means that many times these types of attacks do not require any action by the victim. All it takes is an attacker with sufficient technical knowledge and a vulnerable computer connected to the network.

Origin of the attacks

Generally, these attacks come in two forms: through automatic attacks or through targeted attacks.

Automatic attacks

An automated attack refers to those attacks in which the attacker, instead of actively looking for a victim to attack, puts an automatic system that looks for known bugs in the software of all machines connected to the Internet. This systematic attack aims to identify these vulnerabilities and, once found, notifies the attacker indicating the list of vulnerable equipment that has been found. Once this is done, the attacker takes advantage of this vulnerability to take control of the computer that has the vulnerable software.

As it can be seen, these types of attacks are not aimed at anyone in particular, but are aimed at users with vulnerable applications regardless of who they are and what they do.

Targeted attacks

Another significant type of attack that takes advantage of software bugs is when an attacker fixes on a victim and, once he has decided to attack him, performs a custom analysis where all of his public resources are studied. Once they have all been identified, what is known as the "attack surface" is seen, which refers to the set of attackable resources of an individual or company. Once this attack surface has been identified, a study is made of which system is being used and a personalised attempt is made to attack each of these resources. At this point, the security and configuration of all the infrastructure that the victim has in the system is tested.

Targets exploiting vulnerabilities in applications

Although there are many possible classifications of ways to take advantage of vulnerabilities, one of the most relevant is the one that considers the victim of the attack, which can mainly be an end user, or the service itself offered by a company.

Attacks against users

Generally, this type of attack benefits from incorrect actions performed by users taking advantage of problems in the application they use. In this category there can be, for example, problems with a browser or problems with business applications, such as Microsoft Office or others.

Here, the goal is to make the user perform some action that causes the application in question to behave incorrectly.

A classic example is when the victim opens an attachment they received from an email. This attachment contains a Word document with content forged by an attacker that causes the application to behave inappropriately, for example by opening a connection to the outside that allows the attacker to take control of the victim. This is known as a backdoor attack.

Another classic case is when a malicious attacker gets the victim to open a link to the browser, which is forged in such a way as to steal the browser's cookies, which in practice means that the attacker will have access to all online resources that the victim accesses from that browser.

As can be seen, this type of attack, contrary to what has been presented in automatic attacks, requires specific user action.

To give us an idea, since the creation of the Google Chrome browser in 2009, a total of **3,243 vulnerabilities**,[3] have been found, of which, in the first 8 months of 2023, there have been a total of **31**. This does not mean that this browser is poorly implemented, what it means is that it is one of the most widely used, and therefore there is a lot of interest in finding bugs in it that allow attackers to succeed in their attacks.

Attacks against services

In the case of attacks carried out against services, the aim is generally to obtain the data behind the particular service, but the big difference with attacks against users is that in this case the victim does not have to carry out any action. What the attacker seeks in these cases is to send invalid data to the service or analyse its operation looking for some bad configuration that allows them to access the system.

Sending invalid data usually causes the application to malfunction, which, in some cases, can provide full access to the attacker, these types of vulnerabilities have the same impact as those of attacks against users, in the sense that they are programming errors that could be fixed. Again, the more well-known and used an application is, the more bugs are found in it and the more potential impact they have on our systems.

There are examples of this type of attack with content managers (known as *Content Management Systems – CMS*) which are applications that allow non-expert users to easily enter websites to manage their content. These systems have always been the focus of attacks, as they are present almost everywhere; one of the most famous is WordPress, which, since its creation in 2003, has been reported to have a total of **6,830** different vulnerabilities, some of which have had a media impact, such as the case of the Panama Papers,[4] which in 2016 led to what is known as the biggest journalistic leak in history.

However, it should be noted that, as with attacks against user applications, the companies behind these applications generally have large teams of developers dedicated exclusively to fixing these bugs in the shortest possible time.

As for system configuration errors, there typically are systems with default or very easy-to-guess passwords, administration pages accessible to everyone, or unnecessary services with open access for potential attackers.

Types of vulnerabilities by seniority

The last classification that will be shown in this document is the classification of vulnerabilities according to age. This is particularly important, since, in practice, to be able to fix a problem, its existence must be known. Therefore, a distinction is made between two types: known – or "old" – vulnerabilities and zero-day attacks (*0-day*), which are the vulnerabilities that are not yet reported and therefore not yet known to developers.

[3] https://www.opencve.io/cve?product=chrome&vendor=google

[4] https://www.xataka.com/seguridad/un-plugin-de-wordpress-y-un-drupal-antiguo-causantes-de-la-filtracion-de-los-papeles-de-panama

Known vulnerabilities

There are teams from large and well-known companies, and other freelance experts, who spend their time looking for vulnerabilities. When one is found, it is reported to the developers and they are given some time before making it public. This procedure serves, on the one hand, to force the developers to fix the problems and, on the other hand, to give them enough time so that anyone who does not know about the vulnerability can take advantage of it while it is being fixed. In any case, fixing the vulnerability is not enough; application administrators need to update them to the secure version as soon as possible.

The database of known vulnerabilities is called Common Vulnerabilities and Exposures (CVE)[5] and is a list made by Mitre and funded by the United States government. It currently has a total of **211,265** entries from all existing applications and since the creation of the database in September 1999.

0-day

If known and recorded vulnerabilities can cause us a lot of problems, with zero-day attacks the problem is even greater because, as already mentioned, zero-day attacks are newly discovered vulnerabilities, either by recognised experts or by malicious attackers.

When malicious attackers discover a vulnerability, they can take advantage of the bug found for much longer, since the victim, and the developers of the applications, are not aware of it. So, they are an extremely delicate type of vulnerabilities. There have been famous zero-day attacks throughout history, but the most well-known recently, as will be seen later in this document, is the Pegasus app, which takes advantage of bugs in the iOS messaging system on the iPhone to download the application completely hidden to the user of the mobile device.

Impact

Along with social engineering attacks, attacks that exploit software vulnerabilities are the most common today. There are numerous studies that try to quantify the impact of this type of attack, but they all agree that the economic and prestige impact on the victim of these attacks is enormous.

In 2023,[6] according to IBM, the average cost in the United States of an attack is quantified at 4.45 million dollars, which represents an increase of 2.3% compared to 2022.

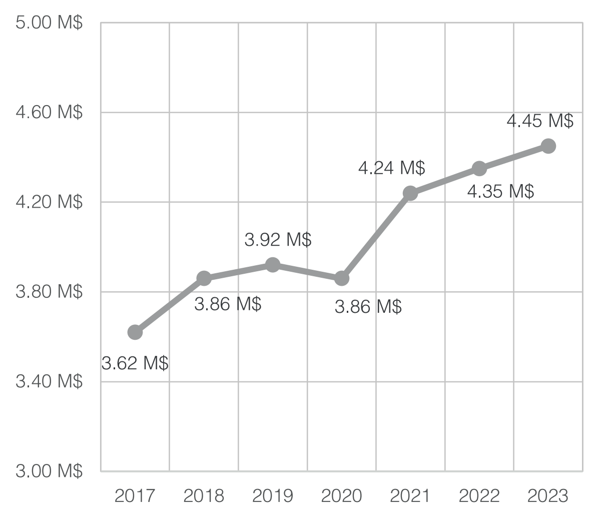

Figure 1: Cost evolution (millions of dollars)

Moreover, the same report makes it clear that on average companies take **182 days** to be aware that an attack has been carried out successfully, and almost **60** to solve the problem. This highlights the great need to have a good cyber security team in the company, as well as knowledge of the tools necessary to be able to mitigate this type of attack and solve them.

An important point to bear in mind is that this economic impact considers, among other things, the impact on the company's reputation, which is generally greatly affected by the loss of customers and the negative publicity it entails, but it also considers the cost of filtering or destroying information that the attacker can carry out. Ransomware attacks will be seen later, which in many cases take advantage of vulnerabilities in applications to gain access to the victim's information.

How to mitigate attacks due to software vulnerabilities

Mitigation of this type of attack can have an impact at various levels. Basically, they can be seen from two points of view, that of the application developer or that of the user (either a system administrator or an end user).

As a developer

Detailing the various development best practices is beyond the scope of this document, but it is important, when using an application, that the user consider the history of the company that provides it. So, things like whether the company is improving the tool and releasing new versions regularly, and also how many critical vulnerabilities have been found in the tool and how long it takes to resolve them should be looked at.

[5] https://cve.mitre.org/cve/

[6] Cost of data Breach Report 2023

As an end user

Strictly as an end user, whether a service administrator or a non-technical end user, the logic is quite similar. As can be seen in vulnerability statistics reports,[7] the vast majority of attacks (75%) are carried out using vulnerabilities reported more than 6 years ago, and in almost all cases the solution would be as simple as updating the application to a stable version. This leads to the great best practice in this aspect: a good user should monitor the status of the tools they use and update them when necessary. This is not easy in principle, so the best way to do it is through the tools provided by the operating system itself, usually in the form of a notification to update either the system or a tool that has been installed, and, as far as possible, to keep the system up to date.

Advanced persistent threats

Before continuing with other attacks, this section is dedicated to how organised crime is increasingly perpetrating cybercrimes that are having a greater impact on people's lives. In particular, this section is dedicated to discussing Advanced Persistent Threats (APT).

What are APTs?

APTs are organised groups of cybercriminals, often autonomous with complex business structures, often financed by governments and with very diverse objectives, but generally with economic or political motivations in order to bring the war to the cyber level.

The actions these groups usually take are generally to steal, spy, or simply disrupt a service, team, or company.

Generally, in attacks carried out by these types of groups, the victim is carefully selected, studied, and only when sufficient information is available do they go on the offensive. It is important to note that an attack carried out by an APT is not a fast attack. This type of threat can last days, weeks or even months, during which the attacker first studies the victim. Once possible vulnerabilities have been found, a Land and Expand attack plan is drawn up. The aim of the plan is to first take control of part of the infrastructure in a stealthy way, but gradually expand until it is considered that all the victim's resources have been taken control of and a coordinated attack is made. At this point, depending on the objective of the attack, several things can happen, but typically, and as will be seen later in ransomware attacks, services provided by the victim are disabled and all data is encrypted and, if possible, the backup copies. Once this point is reached, the victim is informed of the attack and of the steps that must be taken in order to recover the information. Usually, the recovery goes through payment using Bitcoin or other crypto currencies to avoid being found by the relevant authorities.

Generally, organised cyber terrorist groups of this type do not attack the victim again once the ransom has been paid, purely for marketing purposes, and in some cases, they even give them ideas on how to improve the security of their system.[8] The main objective is to ensure that future victims have no hesitation in paying the ransom, given the seriousness of the attacker. This point of prestige has been one of the biggest changes since this type of organised cybercriminals have existed.

With these organised cybercrime groups, what can be seen is that some governments see them as another form of attack against their enemies and use them when necessary for political ends and to shake the stability of the countries attacked.

APT groups

APT groups are constantly monitored by companies and authorities. More than 250 have been identified, among which, at any given time, there may be around 50 actives. In order to identify them, they are usually given a name with the format APT[Number], where, for example, APT1 corresponds to *PLA Unit 61398*,[9] a Chinese cybercriminal group. In addition, each group knows itself by some kind of pseudonym, for example *Double Dragon*[10] (aka APT41), Winnti Group, Barium or Axiom.

This diversity of names is due to the evolution of these groups, which change members or *modus operandi* and they call themselves using different names, sometimes for marketing purposes, sometimes to mislead the authorities.

By country, China has the most APT groups, followed by Russia and the countries of the East, although there are also APT groups in the United States. A key point is that, given the good financing of these groups, many of them now have members all over the world, where they hire them via the dark web and pay them with crypto currencies to avoid monitoring.

[7] https://www.getastra.com/blog/security-audit/cyber-security-vulnerability-statistics/

[8] Ransomhouse group

[9] https://en.wikipedia.org/wiki/PLA_Unit_61398

[10] https://content.fireeye.com/apt-41/rpt-apt41/

Ransomware

Ransomware attacks are undoubtedly one of the most media-driven types of attack due to the large increase in attacks on businesses[11] and public institutions[12, 13] who have suffered from them.

However, ransomware is actually only the last stage of a previous attack to gain access to a system. This is generally done through social engineering or through vulnerabilities in existing applications of the attacked entity.

Ransomware is then an attack where, once the attacker has gained access to a system, they encrypt all the victim's important data using a very strong cryptographic key and demand a ransom for the data. Sometimes, the threat is made to filter and publish the data on the dark web or through other methods, such as Telegram, in order to force the ransom to be paid, all with the aim of obtaining economic or political gain.

It should be noted that both social engineering and application vulnerabilities seen above are in many cases types of attacks perpetrated by attackers who usually have no particular interest in the site or person being attacked; in many cases they don't even know who it is and find the victim using automatic mechanisms. In the case of ransomware, in general, the attack is different: it is usually carried out with a very clear objective, where the victim has been consciously chosen by an APT.

Features and impact

The vast majority of attacks that end up with ransomware tend to use a fairly similar attack vector. In general, the victim is investigated first, both from a technical point of view, looking at externally accessible digital resources, especially those with potential vulnerabilities, and from a social point of view, investigating and trying, through of social engineering, to obtain credentials that allow the attacker to initiate control of the victim's infrastructure.

Once control of a company resource has been achieved, the next step is generally based on trying to expand this control to other resources. This is usually done through privilege escalation systems, that is, the attacker becomes the administrator and, when possible, the administator of the entire domain, thus expanding control. Once the attacker has control over a large part of the systems, a coordinated attack is carried out, that generally consists of two parts: the first is the extraction of data to an external team and the second is its subsequent encryption, if even possible of the backup copies to make the restoration of the information more complicated.

Once the system has been encrypted, the victim of the action is notified and given a link to make a payment that will give them access to the data again and restore the system to its original state. Usually, this message also contains the threat that, if the ransom is not paid, the data will be published.

Even so, distrust of the attacker means that the victim often does not want to make the payment, which has led the attackers, in many cases, to change their business model: they now slowly filter the information that is published about the victim, thereby maximising profit. This is becoming increasingly common, since in recent years, as shown in Figure 2, the amount of victims paying the ransom has been decreasing.

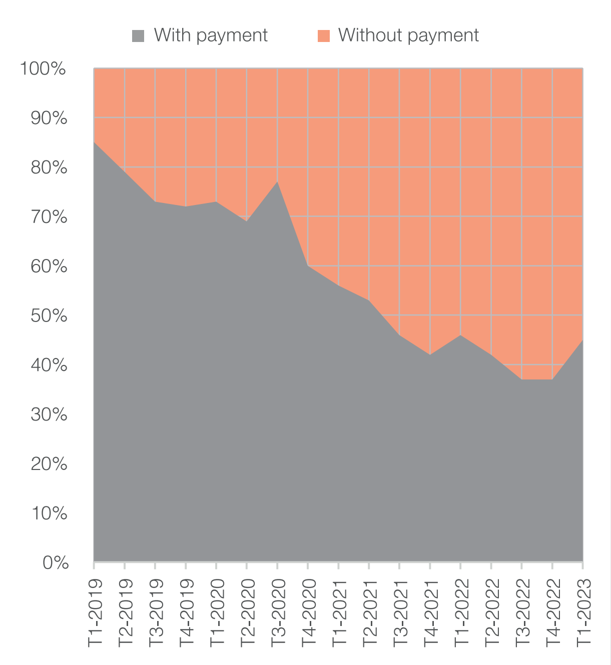

Figure 2: Evolution of payments to cyber criminals for ransomware [Source]

It should be noted that a ransomware attack has two important characteristics, on the one hand it uses other previously seen mechanisms to carry out the attack, and on the other hand, it is generally carried out by organised cybercriminal groups.

How to mitigate ransomware attacks

This type of attack is one of the most difficult to avoid, mainly because there is an organised team in the back-

[11] Cyberattacks on Catalan companies

[12] IT attack at the UAB

[13] https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona

ground with extensive knowledge and a lot of tools to identify and exploit possible errors or vulnerabilities in the system.

Even so, a set of best practices that can minimise the possibility of being violated should be taken into account:

- Make and validate backup copies, always keeping one of them offline to avoid encryption
- Make users aware of the use of digital resources:
  - Have a good password policy
  - Be observant with fraudulent emails
  - Monitor who is given access to resources

Political impact of ransomware attacks

Initially, cyberattacks were a reason for prestige among malicious actors. With the advent of ransomware, the shift towards a business model where attacks could quickly turn a profit was quickly seen. Even so, given the high specialisation and knowledge of APTs, a change in motivation in attacks is being seen, where the economic part is often secondary compared to the destabilisation caused by the attack itself, especially when the cybercriminal group has government funding or other types of advantages, such as protection from extradition, as Russia is well known to do.[14]

This paradigm shift means that nowadays the targets of security programme attacks are universities, hospitals or other critical infrastructures, with the aim of destabilising governments or helping in military matters, as can be seen with the invasion of Ukraine, where the number of cyberattacks after the first offensive increased by a factor of 2.5 against Ukraine and by a factor of 3 against NATO countries.[15]

All in all, this paradigm shift should make governments think about investing in training for citizens in order to try to mitigate as much as possible the impact of this new business model.

Pegasus

Although Pegasus has had a very important media coverage for some time now, it is not a computer attack *per se,* but, as with the vast majority of tools, it can always be misused. This document gives an objective view of Pegasus, its features and how far it can go, without making any judgements about whether it is legitimate for an individual to use it.

Features

Pegasus is a tool known as an information gathering, created by an Israeli company called NSO Group, which is dedicated to achieving device intelligence. In this sense, Pegasus has been designed by experts in cyber security and is sold to governments to be able to perform espionage on criminals and people who can potentially endanger national security. It is not a system designed to be used with political dissidents who do not have a criminal record.

This is because Pegasus takes advantage of vulnerabilities in Android and IOS (iPhone) operating systems, but it also supports other operating systems such as Blackberry or Symbian (Nokia). However, Pegasus' final objective is to study the device in a personalised way for each of the operating systems and victims, and to install an agent that allows the data on the victim's device to be extracted without the victim's knowledge. Thus, Pegasus is able to send a wide range of information to the attacker. The most important data are:

- Location of the victim: the location can be known at all times
- All application data: emails, images, WhatsApp messages…
- Call log
- Audio of the calls to be played by the attacker

Although the actions carried out by Pegasus are very useful for the attacker, it must be said that the point that makes it unique is the way it infects devices. Pegasus allows it to be installed on virtually any mobile device in a hidden and stealthy way and, while taking advantage of vulnerabilities in each of the devices, it can take control of the system by running as an administrator and, therefore, allowing the acquisition of all relevant system data.

In order to avoid detection as much as possible, Pegasus takes advantage of what are known as no-click vulnerabilities (*0-click*), which are those vulnerabilities that do not require any action on the part of the victim to be infected. The best-known example is an existing vulnerability in the iPhone's MMS messaging system that allows Pegasus to infect this type of device. In fact, such vulnerabilities continue to be found and exploited today.[16]

[14] How the Kremlin provides a safe harbor for ransomware

[15] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/

[16] Blastpass - CitizenLab

The fact that Pegasus leaves virtually no trace on devices makes it extremely difficult to detect by antivirus or other systems; so much so that the system itself has a mechanism to uninstall itself from the device when the attacker decides to do so or when it is about to be detected.

How to mitigate Pegasus-type attacks

Realistically, there is no easy or clear way to mitigate such sophisticated attacks. This is mainly because those who have created these tools are experts in program vulnerabilities and have an enormous amount of resources available to them that make it possible to research and discover many zero-day attacks that end up guaranteeing the infection of new devices.

The side effect of this is that other groups are also potentially discoverers of these security issues and may be exploiting them without the knowledge of their victims.

In any case, users are advised to keep their mobile devices up to date in order to minimise the success of attacks such as Pegasus and, as always, to be wary of all messages received from unknown sources.

Other types of attacks

DoS and DDoS attacks

A denial of service (DoS) attack is designed to overload a system's resources to the point that it is unable to respond to legitimate service requests. A distributed denial of service (DDoS) attack is similar in that it also seeks to exhaust a system's resources, but in this case, it is executed by a large number of computers infected with malware that are controlled by the attacker. These attacks are called *denial of service attacks* because the victim server cannot provide service to those who want to access it. That is, in DoS and DDoS network attacks, the goal is simply to disrupt the effectiveness of the service of the attacked server, through an avalanche of illegitimate requests. Since the site must respond to every request, its resources are exhausted with every response. This makes it impossible for the site to serve users as it normally does and often results in a complete shutdown of the site.

A common way to prevent DoS attacks is to use a firewall that detects whether requests sent to the server are legitimate. Attacking requests can be dropped, allowing normal traffic to flow without interruption. An example of such a large Internet attack occurred in February 2020 against Amazon Web Services (AWS).

Password attacks

Passwords are most people's preferred access verification tool, so discovering a person's or service's password is an attractive proposition for an attacker. This can be achieved through a few different methods, some of them using social engineering techniques.

An attacker can also use a dictionary attack to find out a user's password. A dictionary attack is a technique that uses common words and phrases, such as those found in a dictionary, to try to guess the target's password. An effective method to prevent brute-force and dictionary attacks against passwords is to configure a lockout policy. This blocks access to devices, websites or apps automatically after a certain number of failed attempts. With a blocking policy, the attacker only has a few attempts before being blocked and unable to gain access.

Another password attack possibility is based on the use of keyloggers (*keyloggers*). This is a type of malware designed to track every keystroke and report it to an attacker. Typically, a user downloads software believing it to be legitimate, but it installs a keylogger without the user's knowledge. To be protected from these attacks, it is necessary to run a virus scanner. Antivirus companies keep records of the most common keyloggers and will flag them as dangerous.

Information privacy

Although virtually everyone has a more or less clear idea of what privacy is, there is no definition widely accepted by the academic community. A specific aspect is information privacy, which specifically addresses an individual's personal information and the disclosure of that personal information. In other words, information privacy is "the right of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."

The emergence and progress of information processing technologies, the shift from an analogue to a digital, data-centred world and the tendency to collect and store personal data have highlighted the importance of preserving privacy more than ever before. Today's electronic devices allow human beings to generate and record an extraordinary amount of information in various forms: photos, audios, video clips, electronic documents. In addition, telecommunications networks are increasingly being used for a wide range of activities and services: reading the newspaper, shopping, keeping in touch with others, banking, booking holidays, social networking, online calendar, etc. To all this, there is an increasingly frequent presence of Internet of Things (IoT) devices, which generate a large amount of data for application in different areas. Mobile phones, smart watches, and other wearable devices dramatically increase the reach and speed with which people's behavioural and biometric data are available for processing. In some cases, this data is shared with the knowledge of the affected people, for example, when users post videos, photos or opinions about products and current topics. A much larger amount is inadvertently collected when people browse websites, use location services and similar apps, or simply enter smart spaces enhanced with everything from voice assistants to closed-circuit cameras of television.

Behavioural data is highly descriptive of the individual and highlights a multitude of attributes. They contain strong indicators of routines, habits and also medical conditions and "tics". Known correlations between physiological traits and medical conditions include detection of depression or antidepressant use in facial images, detection of organic insufficiency due to eye (hepatitis) or skin (alcohol abuse, state general physical, and others). This data can also be used to uniquely identify individuals; for example, the way of walking has been used in a very relevant way to identify individuals and reveals individual attributes such as age, gender and physiological conditions.

Another privacy threat may come from the use of wearable devices for location-based services (LBS) or health monitoring. Body-monitoring devices can collect information such as heart rate, location and trajectory and store it in the device's cloud or local smartphone. Consequently, the protection of privacy becomes increasingly important, since a large amount of private information can be misused by unwanted third parties without the corresponding protection measures and the consent of the users.

Data is considered sensitive if its unauthorised disclosure, access or use could cause harm, prejudice, embarrassment or discrimination to a person. Some privacy regulations, such as the European Union's General Data Protection Regulation (GDPR) provide specific definitions of sensitive information and require organisations to incorporate appropriate measures to protect such data, such as encryption, access controls and data minimisation.

The study of privacy can be divided into two categories: content privacy and interaction privacy. In the first class, attackers can identify a person from a set of data that has been anonymised or encrypted with certain knowledge about the people concerned. In the second case, while an online activity is carried out, even if the confidentiality of the information transmitted is protected by encryption, the origin and destination of the communication are easily traceable. Information about who communicates with whom may reveal critical information that could be used. For example, someone who accesses a website with information about a life-threatening illness may not get health insurance or lose their job if that information reaches the insurance company or employer. The ability to link all traffic information generated by an Internet user (for example, via IP address, national identification number or social security number) allows for sophisticated profiling of each user.

Thus, a balance needs to be established between the need to use personal data and the right of individuals to data privacy. Data privacy is closely related to data protection. Data privacy and data protection share the same goal: protecting sensitive data from breaches, cyber-attacks, and accidental or intentional data loss. However, while information privacy focuses on rules about how organisations can collect, store and process personal information, data protection focuses on security controls that ensure confidentiality, integrity and availability of information. In addition, data protection often involves protecting not only personal information, but other business-critical data, such as company trade secrets and financial data..

Date types and sensitivity

In order to explore the different types of sensitive information that various regulations define and monitor, it is first necessary to introduce the basic concepts of *personally identifiable information* (PII) and of *personal information* (PI).

PII or personally identifiable information is defined as information that, either alone or when combined with other information, can be used to identify or trace the identity of an individual. PII is the most commonly available and least regulated type of data. In more general terms, the NIST (National Institute of Standards and Technology), in the *document Guide to Protecting the Confidentiality of Personally Identifiable Information*, provides the following examples of information that may be considered PII:

— Name: Full name or alias.

— Personal identification number: such as national ID number, social security number (SSN), passport number, driver's licence number, tax identification number, patient identification number or financial account or credit card number.

— Address data: such as postal address or email address.

— Personal characteristics, including photographic images (especially of the face or other distinguishing characteristic), X-rays, fingerprints or other biometric images or template data (e.g. retina scans, voice signature, facial geometry).

— Information about a person linked or linkable to one of the above (for example, date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, educational information, financial information).

PI or personal information is a broader category. In other words, all PII is considered PI, but not all PI is PII. Thus, PI is defined as that information that identifies, refers to, describes, can be associated or could reasonably be linked, directly or indirectly, to a specific person. PI, therefore, can include data that is obviously associated with an identity – such as a name or date of birth, which is often also PII – or be interpreted in an extremely broad legal way. PI can and usually includes aspects such as racial or ethnic origin, political affiliations or opinions, religious or philosophical beliefs, union membership, sexual orientation, criminal history, medical or genetic information, biometric data, location reports, IP addresses, etc.

It is also useful to outline what types of data are NOT subject to data privacy concerns. There are two main types:

— Non-Sensitive Personal Information (PII): information that is already in public records, such as a telephone directory and online directory.

— Non-Personally Identifiable Information (non-PII): data that cannot be used to identify an individual. Examples include device identifiers or cookies. However, some privacy laws consider that even cookies could be considered personal data, as they can leave traces that could be used in combination with other identifiers to establish a person's identity.

The definition of sensitive information – also known as "sensitive data" – is somewhat different depending on the applicable privacy laws. As a global definition it can be assumed that sensitive information is that personal data that most jurisdictions consider should be treated with a higher standard of care. Data is considered sensitive if its unauthorised disclosure, access or use could cause harm, prejudice, embarrassment or discrimination to a person. Sensitive information often includes personally identifiable information as well as financial, medical, criminal history and any other data that can be used to identify or trace an individual. PII may or may not be sensitive – or may be considered sensitive only in certain circumstances. For example, some PII such as names, telephone numbers or other information that may be in the public domain is not usually considered sensitive (although it might be in certain contexts), while other PII such as social security numbers, alien registration numbers would be. Some privacy regulations, such as the European Union's General Data Protection Regulation (GDPR), provide specific definitions of sensitive information and require organisations to incorporate appropriate measures to protect such data, such as encryption, access and data minimisation.

Therefore, sensitive data requires a higher level of protection due to its sensitive and personal nature, such as medical information, sexual orientation, religion, race, among others. More rigorous security measures are needed to protect it. And, depending on the law, different types of consent may be required to collect it.

Below are some of the types of information commonly considered sensitive, both by the general public and by legal mandates:

— **Personal Health Information** (PHI): medical history, insurance information, and other private data collected by health care providers that could be linked to a particular individual.

— **Personally Identifiable Financial Information** (PIFI): credit card numbers, bank account details or other data relating to a person's finances.

— **Academic files**: grades, academic records, class schedule, billing information and other records relating to an individual's academic education.

The records of a database can contain information, which, according to its nature or typology, can be classified into:

— **Key attributes or identifiers**: are fields that uniquely identify the subjects of the data (name, ID, passport number, telephone, etc.). This type of data must be removed from anonymised records.

— **Quasi-identifiers**: are fields that, although by themselves and in isolation do not identify an individual, (such as age, occupation, postal code) grouped with other quasi-identifying attributes can unambiguously point to a subject. The anonymity techniques work on this data, removing fields that are not necessary for the treatment (in application of the minimisation principle), aggregating or generalising them.

— **Sensitive attributes**: are the fields that contain data that could have a greater impact on the privacy of a specific individual, including special categories of data, and that must not be linked to the data subject to whom they belong (diseases, medical treatments, income level, etc.). This information may be of great interest to the object of the data processing, but, unless there is a justification for this, it must remain dissociated from a specific subject.

- **Others**: information that does not belong to the three previous categories.

Here are some measures to deal with sensitive data from a privacy point of view:

- **Data minimisation**: it is about collecting only the necessary and relevant data for the specific purpose of collection. In other words, only the data necessary to fulfil a specific purpose must be collected and no more than necessary.
- **Informed consent**: it is important to obtain the explicit and free consent of the person to collect and use their sensitive data. Consent must be informed, specific and granted voluntarily.
- **Data protection**: sensitive data must be stored and properly protected to prevent unauthorised access or inappropriate use. Technical measures, such as encryption, and organisational measures, such as security policies and restricted access to data, may be used.
- **Data deletion**: it is important that sensitive data is securely deleted once it is no longer needed for the purpose for which it was collected.
- **Accountability and transparency**: organisations handling sensitive data must be transparent about data collection, use and protection, and must take responsibility for ensuring data privacy and security.

In short, processing sensitive data from a privacy perspective requires specific protection and security measures, as well as transparency and accountability on the part of the organisations that handle this data.

In recent years, privacy preservation has aroused considerable interest among the whole community and therefore also among academics and designers. Consequently, various methods have been developed to protect privacy or policies with a wide scope have been established for the protection of sensitive data. At present, there are no generic solutions that can handle all privacy concerns related to protecting sensitive information from unwanted disclosure while preserving the usefulness of the data. Traditional techniques relied solely on anonymisation, i.e. removing all identifiers – attributes that unambiguously identify participants, such as social security number, passport, first and last name). However, it should be noted that unique combinations of attribute values can be used to unambiguously re-identify an individual in a database without explicit identifiers, and when re-identifying a participant from a database of data, confidential (sensitive) attributes such as salary, illnesses, ideology, etc. may be revealed.

Privacy-Enhancing Technologies

Privacy-Enhancing Technologies (PET) are a set of technical tools designed to protect the privacy of personal data in various applications and information systems. These technologies provide a set of mechanisms to minimise the amount of personal information that is collected, processed and disclosed, ensuring that fundamental privacy principles are met. In the last decade, numerous PET tools have been proposed related to network traffic anonymisation (e.g., the TOR network), identity management, anonymous data storage, in addition to cryptographic and separation of information.

Basically, data privacy techniques can be classified into data perturbation techniques and masking or anonymisation techniques, as indicated in the following figure. Broadly speaking, it is about removing or modifying certain personal data of a person, from a set of data, so that the person cannot be identified directly or indirectly from this data. In this way, the risk of the data being used inappropriately or disclosed without authorisation is reduced. This process is carried out through various techniques, such as the elimination of certain data fields, the replacement of real data values with fictitious values, or the aggregation of data into more general categories.

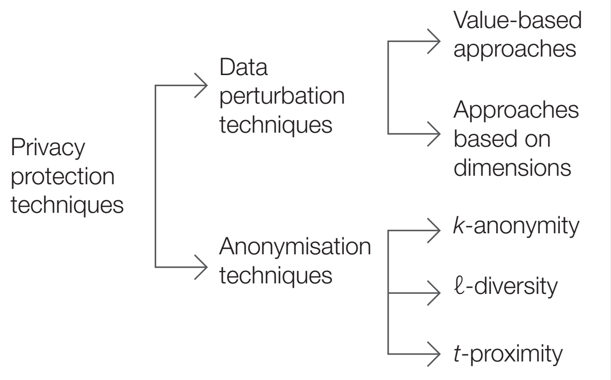
Privacy protection techniques
Data perturbation techniques
Anonymisation techniques
Value-based approaches
Approaches based on dimensions
k-anonymity
ℓ-diversity
t-proximity

Figure 3: Techniques to protect privacy

Data perturbation techniques are a set of methods consisting of introducing deliberate changes to data before its analysis or disclosure. These techniques are particularly relevant in the context of data science, machine learning and data mining, where the aim is to use data to obtain valuable information without revealing sensitive or identifiable information about the individuals or organisations involved. The result is equivalent to adding “noise” to databases that allows individual record confidentiality. Data perturbation is typically applied to electronic health records (EHRs) to protect sensitive information, although its use is not limited to the healthcare industry.

These perturbation techniques can have two different approaches: value-based and dimension-based.

- Value-based approaches refer to methods that modify or perturb data values while preserving general statistical properties or characteristics of the data set. These techniques make it difficult to re-identify specific individuals in a data set, but still allow meaningful information and insights to be gained from the perturbed data. Basically, instead of using the original data values directly, value-based approaches modify those values in a way that preserves the usefulness of the data for analysis but reduces the risk of privacy violations. Value-based approaches are often used in scenarios where data needs to be analysed at the individual level while protecting privacy. Examples include medical research, census data analysis, and machine learning applications. These techniques help organisations and researchers adhere to privacy regulations and ethical standards while gaining valuable insights from sensitive data.
- Dimension-based approaches refer to methods that focus on perturbing or altering the data on specific dimensions or attributes of the dataset, while preserving the overall structure and statistical properties of the data. These techniques are used to improve privacy protection by adding noise or making modifications to certain features, thereby reducing the risk of re-identification of individuals. Among other possibilities, randomisation techniques can be used to introduce controlled noise or alterations to selected dimensions, making it more difficult to link specific data points to individuals while allowing meaningful analysis. Dimension-based approaches are particularly useful when working with datasets where only a subset of attributes contain sensitive information, and it is essential to protect these attributes while allowing analysis in non-sensitive dimensions. These techniques strike the balance between privacy preservation and data utility, ensuring that meaningful insights can still be gained from perturbed data while reducing the risk of privacy breaches.

Anonymisation techniques for privacy refer to methods and processes used to remove or hide personally identifiable information (PII) from data sets, making it more difficult to identify or link specific individuals to the data. However, it should be noted that the effectiveness of these techniques depends on several factors, such as the quality of the anonymisation process, specific privacy requirements, and the threat model. In some cases, even well-anonymised data can be vulnerable to re-identification attacks if other external information is available to attackers. Some types of anonymisation techniques are indicated below.

- ***k*-anonymity**: *k*-anonymity is a data privacy technique used to protect the identity of individuals in publicly shared data sets. The main idea behind the *k*-anonymity is that an entity publishing a data set must ensure that each individual in the data set is indistinguishable from at least *k*-1 other individuals in the same data set. In other words, the *k*-anonymity ensures that a specific individual cannot be identified in a shared data set. An individual is said to be *k*-anonymity within the data set in which it is included if, and only if, for any combination of the associated quasi-identifying attributes, there exist at least one other *k*-1 individuals who share with him the same values for these same attributes. It should be noted that the *k*-anonymity does not focus on the sensitive attributes of the records, but rather on the quasi-identifying attributes that can allow links.

  To apply the technique of *k*-anonymity, data is grouped by attributes that allow a person to be identified, such as name, address, personal identification number, etc. Then, the identifying attributes are removed and the data is grouped into sets containing at least *k* individuals that share the same set of attribute values. To guarantee the *k*-anonymity, generalisation, grouping or data deletion techniques can be used.

  For example, assuming a patient dataset that includes information on age, gender, city of residence and the result of a medical test. To apply the *k*-anonymity, the data could be grouped by age, gender and city of residence, and then remove identifiers such as names or personal identification numbers. Then, certain values can be generalised or suppressed to ensure that each group contains at least patients who share the same set of values for age, gender and city of residence.

  Assuming a hospital has a patient database that includes their ID, information about their age, gender, postcode and disease:

DNI (ID Document)	Age	Gender	Postcode	Illness
21057841	22	M	25036	Cardiovascular
74323432	23	M	25012	Respiratory
23489343	18	M	25600	Cardiovascular
44648948	47	F	08870	Osteoporosis
78489455	42	F	08630	Respiratory
61154615	50	F	08292	No illness
54687897	23	M	17256	Pancreas
87879873	25	M	17800	Paget’s
91584168	19	F	17424	COVID
21548710	41	F	43008	Glaucoma
33728590	41	M	43001	Diabetes
09342859	41	F	43004	No illness

To apply the *k*-anonymity aggregation technique to this table, this procedure could be followed:

- **Set the value of *k***: *k* represents the level of anonymity that is desired, that is to say, the minimum number of individuals that must be present in each group of identifying attributes so that it is not possible to identify any of them. In this case, it is assumed that a level of anonymity is desired *k*=3.
- **Remove identifying attributes** (in this case the DNI) and identify the quasi-identifying attributes: these are those attributes that, combined, can allow the identification of an individual in the original table. In this case, these are age, gender and postcode.
- **Group the data**: the data must be organised by each combination of identifying attributes, so that from the disease it is not possible to identify who the patient is, and that at least there are *k* possibilities.

Age	Gender	Postcode	Diagnosis
<25	M	25***	Cardiovascular
<25	M	25***	Respiratory
<25	M	25***	Cardiovascular
40-50	F	08***	Osteoporosis
40-50	F	08***	Respiratory
40-50	F	08***	No illness
<25	*	17***	Pancreas
<25	*	17***	Paget's
<25	*	17***	COVID
41	*	4300*	Glaucoma
41	*	4300*	Diabetes
41	*	4300*	No illness

Interest-sensitive columns cannot reveal information that has been trimmed in generalised columns. For example, some diseases are unique to men or women, which could reveal a gender attribute that had been cut out, and thus could compromise anonymity.

Values in sensitive columns are not all the same for a particular group of *k*. If the sensitive values are all the same for a set of *k* records that share quasi-identifying attributes, then this set of data is still vulnerable to an attack known as a *homogeneity attack*. In a homogeneity attack, the attacker uses the fact that it is sufficient to find the group of records to which the person belongs if they all have the same sensitive value. For example, if all men over 60 in the data set have cancer; if it is known that Joan is over 60 years old and is in the data set, it is certain that Joan has cancer. Also, even if not all values are equal for a group of *k*, if there is not enough diversity, there is still a high probability that something more will be learned about John. If approximately 90 percent of the records in the group have the same sensitive value, an attacker can infer with high certainty what the person's sensitive attribute is. Measures like ℓ-diversity and the *t*-proximity (which will be explained later) can be used to specify that between any *k* matching records there must be some amount of diversity in the sensitive values. To illustrate this, imagining that the three people in the last block had had the same disease, if it is known that one of the people in that study lives in the 43004 postcode, it can already be known which disease they have and, therefore, their privacy would have been compromised.

- **ℓ-diversity:** this concept was introduced to avoid the homogeneity attacks indicated in the previous paragraph. The ℓ-diversity is a technique that allows to expand the *k*-anonymity ensuring that each group of indistinguishable records has at least ℓ different values for sensitive attributes. This adds an additional layer of protection against attribute-based attacks. It proceeds to illustrate the ℓ-diversity with an example. Assuming that a data set contains the medical records of patients, and one of the attributes is "Diagnosis", which indicates the medical condition of each patient. It is intended to release a portion of this data set for research purposes while preserving patient privacy.

Assuming that the original data set is

Age	Gender	Postcode	Diagnosis
29	M	90216	Diabetes
29	F	90219	Asthma
31	M	90217	Asthma
22	F	94105	Hypertension
39	M	94117	Asthma
24	F	94109	Asthma
37	M	94126	Diabetes
26	F	90216	Diabetes
21	M	90213	Diabetes
36	M	94105	Hypertension
27	M	90217	Hypertension
28	F	90211	Hypertension
22	M	90211	Hypertension
34	M	90211	Hypertension
23	F	94102	Diabetes
32	M	90213	Diabetes
24	M	90218	Asthma
28	M	90214	Asthma

a possible modification of the database after applying the ℓ-diversity with ℓ=3, would be

Age	Gender	Postcode	Diagnosis
30-34	M	9021*	Diabetes
30-34	M	9021*	Hypertension
30-34	M	9021*	Asthma

Age	Gender	Postcode	Diagnosis
20-24	F	9410*	Hypertension
20-24	F	9410*	Diabetes
20-24	F	9410*	Asthma
25-29	F	9021*	Hypertension
25-29	F	9021*	Diabetes
25-29	F	9021*	Asthma
35-39	M	941**	Hypertension
35-39	M	941**	Diabetes
35-39	M	941**	Asthma
20-24	M	9021*	Hypertension
20-24	M	9021*	Diabetes
20-24	M	9021*	Asthma
25-29	M	9021*	Hypertension
25-29	M	9021*	Diabetes
25-29	M	9021*	Asthma

– In this modified data set, a 3-diversity has been ensured for the "Diagnosis" attribute. For the "Diabetes" category, there are five different patients. This makes it more difficult for an adversary to determine the medical condition of a specific individual based solely on the shared "Diagnosis" attribute.

– The ℓ-diversity is a way to strengthen privacy protection of sensitive attributes within a dataset, particularly when data is released or shared for research or analysis, while reducing the risk of inference-based attacks in attributes. The specific value of ℓ in the ℓ-diversity may vary depending on the desired level of privacy protection and the nature of the data set.

— ***t*-proximity**: The *t*-proximity is a privacy measure that aims to ensure that the distribution of sensitive attributes in a group of indistinguishable records is not significantly different from the general distribution in the dataset.

Privacy in the life cycle stages of the information

Privacy techniques and mechanisms vary according to the phase of the data life cycle. The following is a presentation of the techniques and mechanisms of privacy in the phases of data collection, data generation, processing and processing:

Stage 1: Collection of personal information

The first stage of the information life cycle is the collection of personal data. Here, entities must ensure that they obtain appropriate consent from individuals before collecting their data. In addition, clear and transparent policies must be established to inform users about how their personal information will be used.

Stage 2: Storage and management of personal information

Once personal information is collected, it is crucial to ensure its safe storage and proper management. This involves implementing technical and organisational measures to protect data against unauthorised access, loss or leakage. In addition, it is essential to establish clear policies and procedures about who has access to personal information and how it is managed internally. Among other techniques, the following are used:

— **Encryption:** Encrypting data involves transforming it into a sequence of characters that is unintelligible to anyone who does not have the decryption key. This helps protect stored data in case it is stolen or accessed in an unauthorised manner.

— **Restricted access:** Measures can be put in place to limit access to stored data to only authorised individuals. This includes implementing authentication and authorisation systems to ensure that only authorised individuals have access to data.

Stage 3: Use and processing of personal information

During this stage, organisations use the personal information collected for the intended purposes. However, it is important to ensure that the use and processing of data is carried out in a manner compatible with applicable privacy laws and regulations. Organisations must establish appropriate restrictions and controls to ensure that personal information is only used in accordance with the consents given by individuals. Among other techniques, the following are used:

— **Anonymisation or perturbation:** the collected data sets are modified for publication ensuring privacy. This allows the processing of data for specific purposes without revealing the identity of the individual.

— **Data minimisation:** as mentioned above, data minimisation involves publishing only the information necessary for the specific purpose of use.

Stage 4: Retention and deletion of personal information

The retention and disposal of personal information is a critical stage in the information life cycle. Entities must define clear retention periods and comply with legal and regulatory obligations. In addition, they must implement appropriate procedures to securely and permanently delete personal data when it is no longer necessary for the purposes for which it was collected.

In summary, privacy techniques and mechanisms in the phases of data generation, storage and processing include anonymisation, perturbation, data minimisation, encryption, restricted access, informed consent. It is important to implement these measures to ensure data privacy and security at each stage of the data life cycle.

Privacy aspects

There are three types of privacy that can be distinguished: data privacy, user privacy and location privacy. Data privacy, user privacy, and location privacy are distinct but related concepts in the context of online privacy. Data privacy refers to the protection of personal data, user privacy refers to the protection of an individual's online identity, and location privacy refers to the protection of location information of an individual.

In summary it could be said:

- Data privacy refers to an individual's right to control the personal information they share with others. This information may include name, address, phone number, email address, browsing history, purchase history, etc.
- User privacy refers to an individual's right to control their online identity. This identity may include username, password, social media profiles, etc.
- Location privacy refers to an individual's right to control their location information. This information may be collected by government agencies, technology companies or other third parties.

Data privacy

It refers to the protection of an individual's personal data, such as their name, address, identification number, financial information, medical history, among others. Data privacy implies that this data is only collected, stored and used in a legal and ethical manner, and that appropriate measures are implemented to ensure its security. Data privacy focuses on protecting data as an entity in itself.

Some practical examples of data privacy:

- An e-commerce company must obtain a customer's informed consent before collecting personal data, such as their name, email address and payment details.
- A data analysis company must use data anonymisation techniques to remove any information that can identify an individual from the collected data before using it for analysis.
- A financial services company must limit access to personal data to only those employees who need access to perform their job duties.
- An email service must use encryption techniques to protect data as it is transmitted from one server to another.

User privacy

It refers to the protection of an individual's online identity, including their username, password, email addresses and other personally identifiable information. User privacy implies that this information is only shared with third parties with the consent of the user and that security measures are implemented to protect it from unauthorised exposure. User privacy focuses on protecting the user's identity and how it is used online.

Some practical examples of user privacy:

- A social networking website must allow users to set their privacy preferences, such as who can see their profile and who can see their posts.
- A messaging app should allow users to control who can see their contact information, such as phone number or email address.
- An email service should allow users to control who can send them emails and who can see their inbox.
- A video streaming service must allow users to control who can see their viewing history and what content recommendations are shown to them.

Location privacy

Location privacy is an individual's right to control information about their geographic location, location history, and travel patterns. This information may be collected by various devices and applications, including mobile phones, computers, GPS navigation systems and activity tracking applications.

Location privacy is important for several reasons. Firstly, it can be used to track a person's movements, and secondly, location information can be used to create behavioural profiles, and consequently be used for marketing or espionage purposes.

Many of the actions performed over the Internet, such as calling someone on a mobile phone, posting about an event, using a car's navigation system or paying with a credit card, leave an uninterrupted trail of everyday activities. These actions are easily logged and stored persistently in databases. Location privacy requires that this information be collected and shared only in transparent and legal ways, and that users have control over how it is used and shared.

The common practice adopted by data collectors and owners to protect the privacy of the individuals they monitor is pseudonymisation, also known as *depersonalisation*. This simple approach consists of removing all personal identifiers (for example, information that is directly related to the person's identity, such as name, phone number, precise address, number plate number, etc.) and replace them with some pseudo-identifier. Unfortunately, pseudonymisation only provides a very low level of protection, for example, naive cross-correlation of pseudonymised data with additional information (obtained, for example, from publicly accessible social media data) may allow re-identification, it is a say, the disclosure of user identities with a high probability. So, the first step to protect location privacy is to disable the mobile phone's location when it is not needed.

Regulation of data protection

Due to growing public concerns, governments are busy creating and adapting data protection and privacy laws. Indeed, the need to address current privacy issues and protect data privacy rights is a global trend. The EU's General Data Protection Regulation (GDPR) is the best-known law, but many countries, including Brazil, India and New Zealand, have enacted new privacy regulations or strengthened existing laws to regulate how personal data may be collected, stored, used, disclosed and transmitted.

In Spain, the data protection regulation is composed of two main documents:

- The General Data Protection Regulation (GDPR), which is a European regulation that applies to all member states of the European Union, including Spain.
- The Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), which is a Spanish law that enhances the GDPR.

The GDPR is a European standard that establishes a framework for the protection of personal data throughout the European Union. This regulation applies to all companies that process personal data of citizens of the European Union, regardless of the location of the company. The GDPR defines personal data as "all information about an identified or identifiable natural person". This includes information such as name, address, phone number, email address, browsing history and purchase history. The GDPR establishes a series of principles that must be respected by people who process personal data. These principles include:

- Fairness and transparency: Individuals must be informed about how their personal data is processed, and it can only be processed for a specified and lawful purpose.
- Data minimisation: only those personal data that are necessary for the intended purpose may be collected.
- Limitation of retention: personal data may only be retained for the time necessary for the intended purpose.
- Integrity and confidentiality: Personal data must be protected against unauthorised access, modification, disclosure or destruction.
- Liability: Those who process personal data must be responsible for complying with the principles of the GDPR.

The LOPDGDD complements the GDPR and establishes a series of specific measures for the protection of personal data in Spain. These measures include:

- The creation of the Spanish Data Protection Agency (AEPD), which is the body responsible for ensuring compliance with data protection regulations in Spain.
- The right of citizens to request access, rectification, deletion, limitation of processing, data portability and opposition to the processing of their personal data.
- The duty of companies to notify the AEPD of any security incidents that may affect the personal data of their customers.

Additionally, in Catalonia there is a specific control authority, the Catalan Data Protection Authority (APDCAT), which is the entity primarily responsible for supervising and guaranteeing the application of the two aforementioned regulations. It also has other functions such as promoting public awareness and understanding of the risks, rules, safeguards and rights related to processing, and advising, in accordance with the law of member states, the national parliament, the government and others institutions and bodies, on the legislative and administrative measures relating to the protection of the rights and freedoms of natural persons with regard to the treatment of data protection regulations in Catalonia. The APDCAT works in a coordinated manner with the Spanish Data Protection Agency (AEPD) to guarantee effective protection of citizens' rights in relation to their personal data.

Best practice guide

Recommendations have been given throughout the document. this chapter provides a summary of the views and adds a few more, combining both the cyberattacks part and the information privacy part.

General recommendations

It has been seen that cyber security is a complex issue, more attacks are being suffered every day. Although there is no such thing as a completely secure system, applying common sense and following very clear guidelines can help minimise the impact of potential attacks. Therefore, it is recommended to follow these general safety points:

- **Awareness and training**: it is important that people who handle personal data are aware of the importance of privacy and know how to protect it. Employees and users need to be trained in privacy best practices.
- **Source verification**: verify the source before providing personal or financial information, and avoid responding to suspicious emails, phone calls or messages.
- **Privacy in social networks**: it is necessary to review the privacy settings on social media accounts and adjust the options to protect personal information, allowing only what is strictly necessary to be shared.
- **Safe browsing**: it is necessary to use a secure web browser and set it to block third-party cookies and prevent tracking. Also ensure that the websites that are visited are secure and use the HTTPS protocol.
- **Secure email**: it is necessary to use a secure and encrypted email service and avoid sending confidential information via email.
- **Safe online shopping**: it is necessary to verify that the website is secure before making an online purchase, and use a virtual credit card or secure payment service.
- **Identity protection**: it is necessary to keep personal information safe and protect online identity by using tools like credit blocking and identity monitoring.

How to save personal information

As already seen, data and information in general are both the target of system attackers and a concern for online services that are commonly used. Therefore, both when holding data from third parties and when offering a service, the following points must be taken into account:

- **Use of encryption**: both at the level of the data that is transmitted to a recipient and the data that is saved on any storage device.
- **Data minimisation**: it is necessary to collect and store only the information necessary to fulfil the specific purpose of data collection. No need to collect unnecessary data.
- **Informed consent**: explicit and informed consent must be obtained from individuals before data is collected. Consent must be freely given and individuals must know exactly what is being done with their data.
- **Data security**: it is important to ensure the security of personal data by implementing appropriate technical and organisational security measures, such as encryption, user authentication, access control and activity monitoring.
- **Transparency**: it is necessary to inform individuals about the use of their personal data, including who is responsible for the processing of the data, the purpose of the data collection and how the data will be used.
- **User rights**: individuals have rights in relation to personal data, such as the right of access, rectification, deletion, limitation of processing and data portability. It is important to ensure that these rights are respected.
- **Impact assessments**: privacy impact assessments should be carried out to identify and minimise privacy risks in the collection and processing of personal data.
- **Review and update**: privacy policies and practices should be reviewed and updated on a regular basis to ensure that best practices are followed and adapted to changes in regulations and technology.

How to use the devices

While learning how to store data correctly is important, so is how individuals monitor and use their personal devices, which ultimately provide access to the data they want to protect. The following recommendations can therefore be made:

- **Secure passwords**: strong and different passwords must be used for each device and online services account. Passwords must be changed periodically.
- **Two-factor authentication**: it is very convenient to enable two-factor authentication whenever possible. This adds an extra layer of security to protect devices and accounts.
- **Software updates**: devices and applications must be kept up-to-date with the latest software versions and security updates to avoid vulnerabilities.
- **Antivirus and firewall**: it is necessary to use antivirus and firewall programs to protect devices from viruses, malware, and other computer attacks.

- **Secure networks**: connection to open Wi-Fi networks should be avoided as much as possible, as they may be vulnerable to computer attacks.
- **Camera and microphone privacy**: it is necessary to take steps to protect the privacy of the device's camera and microphone, such as covering the camera or turning off the microphone when not in use.
- **Backups**: important data stored on devices should be backed up regularly to protect against loss, theft or device failure.
- **Privacy settings**: device and application privacy settings should be reviewed and adjusted to ensure that personal information is adequately protected and unauthorised access is prevented.
- **Limit of personal information**: it is necessary to limit the personal information that is shared on personal devices, especially on social networks and messaging applications.
- **App permission review**: it is necessary to regularly review the permissions that have been granted to applications and revoke those that do not need access to personal information.
- **Use of VPN or Zero Trust infrastructure**: it is necessary to use a virtual private network (VPN) to encrypt the Internet connection and protect online privacy, especially when connecting from outside the corporate network.

Conclusions

This document has shown the big problems in a summarised way, the big points to take into account both from the point of view of cyberattacks and from the point of view of privacy of the data that are used on a day-to-day basis.

With regard to cyberattacks, what is found is that, more or less actively, a malicious actor seeks to make illegitimate use of a system or steal certain information in order to receive some benefit. It has been seen that the vast majority of attacks focus on social engineering or take advantage of vulnerabilities in existing software in order to appropriate information or systems with errors. As a result of these attacks, it has been seen that there are organised cybercrime groups, known as APTs, which for economic or political reasons carry out attacks aimed at carefully selected victims. These attacks, nowadays, in a very high proportion, are with ransomware, where the attacker aims to extort the victim by encrypting the existing data in their systems and threatening to publish them on the dark web.

Regarding cyberattacks, it has also been shown, although it cannot be considered an attack in itself, the Pegasus system, a cyber espionage software that is used to observe terrorist groups, but which has been in the news in recent times for the evil use made by certain governments.

Regarding data privacy, it has been possible to observe the impact and implications of sharing private data (whether personal or not) on the Internet. It was possible to see what types of data are held according to their sensitivity, and what needs to be done to be able to store and treat them with the appropriate level of privacy. The technologies currently available to protect personal data have also been considered in order to achieve this.

In addition, the impact of privacy on the stages of the information life cycle has also been studied, where it has been possible to see how privacy is important at all levels of information dissemination. The last important point of privacy that has been studied has been the different aspects of privacy that affect information. Thus, it has been possible to observe privacy from the point of view of the data itself, but also considering the users and the location of the data.

Finally, by way of summary, a series of good practices have been presented to try to mitigate as much as possible the presence of cyberattacks on the systems, as well as the procedure that must be followed to ensure that the data published on the network complies with the necessary privacy guarantees.

cap
cit
Consell Assessor
del Parlament
sobre Ciència
i Tecnologia

UPC
UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Cyber security and privacy report for the Parliament of Catalonia

Authors: Miquel Soriano, René Serral-Gracià
Polytechnic University of Catalonia

The Parliamentary Advisory Council on Science and Technology (CAPCIT) is a parliamentary body created in 2008 with the objective of co-ordinating the information and advice on science and technology that members and bodies of Parliament require. CAPCIT is a combined body made up of members of Parliament appointed to the Council and representatives of the leading scientific and technical institutions of Catalonia: the Catalan Studies Institute (IEC), the Catalan Foundation for Research and Innovation (FCRI), the Catalan Scientific Communication Council (C4) and the Catalan Association of Public Universities (ACUP). For further information: http://www.parlament.cat/capcit.