Cyber-space

A lawless world

Internet: the revolution that changed the rules of the game

ÁLVARO ÉCIJA

My name is Álvaro Écija Bernal and I am the Managing Partner of **Ecix Group**, a technology and legal firm that specialises in Cyber-security.

I have dedicated many years to the study and practice of law, and from the moment I stepped into law school up until now I have been lucky enough to study the new problems that arise in cyberspace and the internet in depth.

Cyber-space is a reality that is here to stay. To what extent does the internet open new doors for us? Are we sufficiently protected against cyber-problems? Is it possible to get good legal protection on the net?

The internet is an authentic revolution in which thousands of millions of people, companies and even machines live side by side: what does it take? Knowing it, ordering it and protecting ourselves against cyber-problems.

This is where Cyber-law comes in: a discipline which studies the problems, related to the physical world in which we live, that internet users that surf online are faced with and it provides the necessary solutions to achieve the best protection possible.

At Ciberderecho, we are committed to being pioneers when it comes to talking about these issues and I want this book to be a gateway for knowledge about what can happen to us online and how to avoid it.

You will discover how to understand the internet's cyber-problems, why they occur, how to beat them and how to prevent them.

Cyber-space disrupts usual lawmaking practice. It is not the Law that governs the internet, but the internet that governs the Law.

1 Introduction

Cyber-space is a reality that is here to stay. Thousands of millions of machines, internet users, companies and all types of organisations live within it. Who is missing? States and Governments.

It goes without saying that Cyber-space has become a new digital or virtual world, without physical borders. A new world that cannot stray far from the law and the distinct legal systems that make up our civilised, modern world. But of course, in a world where physical space does not exist (but time does) it is not clear who holds the legislative and judicial power. And so, we face a world of legislative anarchy in which, paradoxically, all types of cyber-societies live together.

In parallel, some states have launched a conquest of the net: some to censor it and others, in the name of national security, to protect its citizens.

Moreover, cyber-space is now the fifth strategic environment, after the land, sea, air and space, although curiously, and unlike the first four, it does not have any type of regulatory arrangement.

But, as the internet seems like a world of social disorder where technical order prevails, I will start at the end by saying that the lawyer of these "new" technologies (which are old for me) or the lawyer of the society of information is a counsel who is a prisoner in his own mind, of his knowledge. The entanglement of laws and the courts' principles of competition make up the bars and limits of his mental prison. A prison which started to be built when studying the legal system which is delimited by the physical boarders of the sovereign State of the country of study.

Without a doubt, the future of this lawyer goes from disconnecting himself, to fearlessly jumping into Cyber-space, freeing himself from the shackles of traditional legal thinking and observing the social conflicts of the digital world with some new "Cyber glasses". This is the only way to find new legal solutions. If the lawyer makes this jump, a new #cyberlawyer will have been born.

When faced with this panorama of "science fiction" and uncertainty, the lawyer of the new technologies or other disciplines should advise his client, trying to give them the most certainty and legal security. And how is this done?

Well, for that a choice has to be made between reading this or continuing in the world of traditional legal systems as we know them today.

2 Structure of the Book: "Two Colours for Two Distinct Yet Connected Worlds"

This book will revolve around the positive regulation (in favour of it) and the negative (no regulation) in terms of the Law in Cyber-space. As Law is a discipline that forms part of what are considered by be social sciences, that means that it is not exact. Needless to say that the ideas presented here may be incorrect should, in the future, they be checked against the true regulatory evolution. But this book does not aim to make exact, scientific assumptions, as Law does not do that either. My intention is to contribute to the research of organisation formulas that help to settle the present problems, suggesting possible solutions based on current tools and legal knowledge.

So, as the title of this section predicted, this book is printed in two colours. Why? Mainly because it is going to deal with legal problems that affect the "physical" world as we know it, but also, it will study the problems that affect another domain: "cyber-space" or the virtual world.

Aspects regarding the first block of problems- the physical world- will be printed in black, whereas those regarding the problems regarding Cyber-space will be printed in blue.

By doing this, with just a quick glance we will be able to distinguish if we are studying an issue in the physical world, from the perspective of the current Law, just as we have learnt it, or if we are facing a new situation from Cyber-space.

In the first part of this book, there will be a discussion of the new world that appeared before our eyes, known to us as the internet: its key characteristics, its new values, the new social agents and the problems that affect Law and the peaceful coexistence between cyber-citizens.

Afterwards there will be a succinct discussion of the key features of the legal system of the physical world (highlighting amongst those the territorial principle of the sovereign states to legally order their territories) and the problems that Cyberspace brings with it.

Continuing on from this, the opportunities that the internet provides to the social agents of the legal world (lawyers, solicitors, professors, judges, etc.) will be addressed, as will the possibility of the birth of a new social agent: the Cyber-lawyer.

Finally, as a way of bringing this first section to a close, the way Cyber-space is organised will be analysed, that is if it is at all, and which proposals of legal systems could be introduced in the near future. Likewise, there will be an analysis of the problems that arise from resolving conflicts via what is known as "electronic evidence".

The second section will deal, one by one, with the problems that affect the Law and that currently happen on the internet, affecting the peaceful coexistence of the citizens and companies that surf on the net. I will refer to these problems as "antisocial conflicts or behaviours".

Each one of these antisocial behaviours will be analysed, differentiating the approach, analysis and a possible proposal for solutions, when possible. In the approach, the factual situation of the physical world which leads to the antisocial behaviour will be rejected so

that after, printed in blue, this behaviour in the world of the internet can be described. Following that, there will be a generic analysis of the key regulations in the sovereign States and subsequently a detailed analysis of its treatment in Cyber-space will be analysed (once again in blue ink). Finally, in the third section current possible solutions will be suggested, with the aim of leaving the scientific debate to future agents of the legal world. Therefore, the proposed solutions aim to explore the beginnings of possible legal pathways and to help to clear the path that others can take and to thus collaborate in the search for better solutions.

Due to the fact that certain antisocial cyber-behaviour, as they occur and are represented in cyberspace, are better understood and more easily explained through other diagrams, on occasions this methodology will give way to a far more vivid and concise explanation.

To conclude, it should be noted that I am facing a new subject and we would even say, a new legal discipline which is, on the whole, unknown. Because of this, to try and facilitate reading, this book will be illustrated with graphs, drawings and diagrams. I am taking this freedom as I understand that we are facing a new world. We stand before a new era, which was preceded by the industrial revolution, in which everything changes at a dizzying speed and I consider that the traditional formula, which is completely valid for subjects of great legal importance and tradition, is not valid when explaining the events in the world of Cyber-space. As the popular saying goes, "a picture is worth a thousand words".

Last of all, the book will end with a topic that has been intentionally chosen to generate debate and that will surely be the object of diverse criticism. This section will suggest the creation of an internet protocol, which I have christened as "ID Protocol" and that, just like the other ensemble of internet protocols, should be embedded in its own TCP/IP protocol with the aim of rectifying a large part of the problems caused by antisocial behaviour on the internet and which are difficult to prosecute, mainly because they are committed anonymously.

3 Internet: A Network in Cyberspace

The Network of Networks (TCP/IP) has caused a true revolution. With that, a new era of information has been born.

Its penetration in society has been far quicker than that of television or radio. Advanced societies have not experienced such a deep and quick change since the Industrial Revolution.

In barely five years, in First World countries, the step has been taken from using computers to help with automated tasks, to every type of device being connected to the internet.

Meanwhile, in intent at not losing their strategic predominance, the governments of the richest countries have launched a conquest of the net.

It is true that on the internet neither governments nor their States have virtual representation as the network lacks geographic boundaries. The same thing happens when we talk about what we today conceive as Legislative and Legal Power.

However, diverse societies or tribes coexist on the network which has been named "the New Society of Information".

In this virtual world, internet surfers, machines, private companies and non-profit organisations coexist.

3.1 A New Virtual World

In this new world, activities for peaceful coexistence are being created, but so too are, and as History shows, attitudes that cause damage or harm other users.

And this is where the Law cannot stay on the sidelines as a mere observer. The known problem is that Law is a social science or discipline which acts where it holds power.

The Legislative and Legal power of the States is deployed with complete efficiency through the respective legal systems, but that is done within their territorial limits.

But the internet is an immaterial, virtual world where physical limits and territories do not exist. A world which is shaping up to be like a "weapon" of power, in which the most technically advanced States (U.S.A., Israel, Russia, China, etc.) want to conquer in order to preserve their supremacy and conserve their political, economical and social power.

That is why the internet, or Cyber-space to be more specific, has become the fifth strategic environment, after Land, Sea, Air and Space.

As we know, the world is divided into Land, Sea and Air. And further from its borders, Space begins. It is unknown, as Stephen Hawking said, whether Space has a limit or if it is infinite. Furthermore, it seems as though Space is constantly expanding and it contains

millions of galaxies, but despite all we know about it, it continues to be one of mankind's great unknowns.

Another scientist, Albert Einstein, revolutionised the concepts of time, space and the concept of reality by affirming that space and time are united. By coming up with that equation (the famous aether in Newton theory), Einstein broke what had been scientifically believed before about how time, on the one hand, moved in a lineal, level way -from backwards to forwards- whilst space, on the other hand, could go in different directions. According to Einstein's model, it does not seem to be like this: both are inextricably linked. Furthermore, gravity affects spacetime, deforming and curving it. Hence, time is understood as a human invention to measure the intervals between events, be that relative and not complete in the whole Universe. That is why time goes slowly in places with more gravity and faster in places with less gravity.

Well then, in the Fifth Environment, Cyber-space, these laws of physics do not apply, as space and matter do not exist, although time does. In other words, in Cyber-space there are (cyber)events but they are not committed in any place on concrete three-dimensional place.

Likewise, in Cyber-space, Laws as we know and understand them, do not apply. Therefore, we could say that this new world raises serious questions, both in terms of Exact Science (Physics) and the Social or inexact Sciences (Law).

And herein lies the problem-opportunity that this manual tries to approach, with the limitation of what the human mind and intelligence is able to humbly encompass in this specific moment and place.

This is what I call the "black hole" of the management of Cyber-space and which, of course, as Stephen Hawking said, is not black, but grey.

And it is within this range of greys where this book delves in, to search for the outlines and limits of where the term "the Science of Law in Cyber-space" should start and end.

PHYSICAL WORLD

CYBER-WORLD

3.2 Characteristics of Cyber-space

For didactic purposes, the following characteristics can be highlighted:

- Immaterial, devoid of matter.
- Without physical borders.
- Without democratic or authoritarian States or Governments.
- Cyber-citizens and Cyber-organisations peacefully coexist inside it.
- Acceptable behaviour and behaviour which is not ethically acceptable for citizens of the other world coexist.
- Some values which are accepted by the majority prevail:
    - The principle of technological neutrality
    - The freedom of speech
    - Devoid of political power, without Governmental interference.
- It seems to lack a legal framework.
- However, there is order, for example, in the assignation of domains and IP numbers. Disputes are settled via arbitration organisations and not via the courts.
- Unfortunately, "criminal" actions as reprehensible as the following also coexist:
    - Child pornography
    - Identity theft
    - DDoS attacks
    - Cyberterrorism
    - Virtual money fraud
    - Intellectual property piracy
    - …

3.3 New Agents: Cyber-citizens, Organisations and Companies- and the States and Governments?

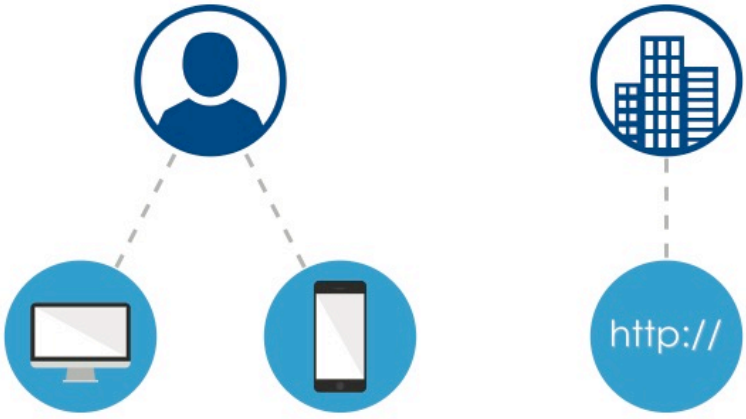
In this area of Cyber-space, two types of key actors can be distinguished:

- The citizens that access the internet through a device or machine (hardware), normally via a telecommunications operator or an ISP. From this moment henceforth they will be referred to as "**Cyber-citizens**".

  These Cyber-citizens surf the net for personal and/or professional reasons and, often, their digital "avatar" does not coincide with the physical world. In other words: what appears on the internet, both personally and professionally, is not always the same as on the other side of the screen.

- The **Organisations and Companies**: that are represented, normally by means of a domain or brand.

The communication of both gives way to a host of variations: customer-provider; consumer-company; patient-doctor; client-lawyer; searcher-advertiser; etc.



- **And the States and their Governments?**

They are not found represented on the internet, despite them seemingly wanting to play a relevant role and from there, the formal declarations of the Strategic Cyber-security Plans, the creation of cells or commands for digital defence-attack and, why not, Cyber-wars and espionage between Physical States.

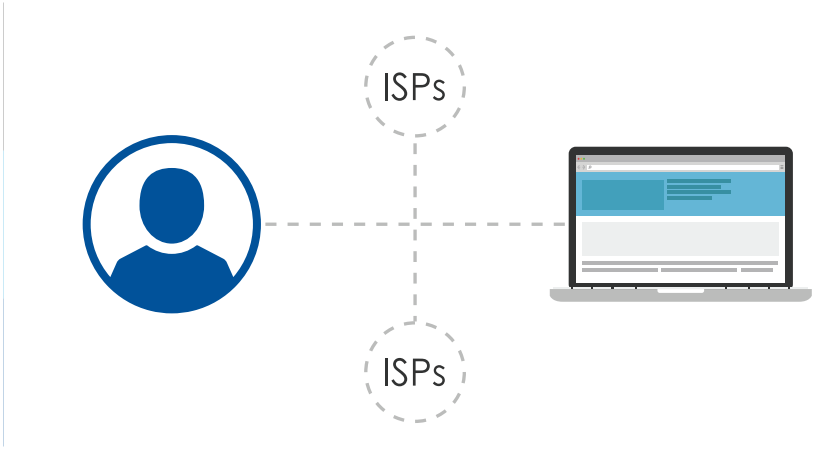
And how is this possible? Because there is a feature that connects the two worlds. An amazing feature that seems like Science Fiction: what happens in one world can affect the other. For example, a prolonged and distributed automatic denial of service attack could stop a thermal power plant and affect the homes of thousands of citizens. And vice versa: a flood could shut down an online shop.

This feature connects, and the same time separates, the two worlds. This defines the entrance-exit, through an ISP, a cable, wave or satellite, separating the real from the virtual. This is what I call the "cyber-border".

The cyber-border separates the cyber-citizens from the machine from which it requests, through a HOST device, the information that another SERVER machines responds to, returning other information to the initial HOST. Hence, the cyber-border separates the citizen's physical machine from what is "behind" it. Or likewise, the physical world is separated from the virtual world that it accesses via a motorway of communication (cable, satellite, waves) and through a standard protocol.

3.4 The "Borders" to Access the Network: The "ISPs"

At a later stage we will see how in this Cyber-border, the States wish to force the ISPs (Internet Service Providers) to convert themselves into customs where entrance and exit information about each cyber-citizen is stored. Furthermore this is done in the name of National Security and let us remember that not long ago, these telecommunication operators where public companies, financed with money collected from taxes and that, furthermore, they occupy a "physical" public and not private space (the air and the pavements, for example).



3.5 The Limits of the Law

It should be pointed out that that main limit that the Law has is the human mind. As has been previously mentioned, Law is an inexact discipline that has been continuously evolving over recent centuries and that has been studied and interpreted by people through assumptions that have been modified, just like the scientific theorems of any other discipline.

Therefore, I dare to say that Law is a discipline that is a perfect as it is imperfect, depending on the observer and the moment in which it is applied.

It is a bit like the theory of relativity. Everything is relative and in movement and, thus, changing.

Because of this, one same event observed by two different "judges" would result in two different sentences, one anterior and one posterior in time, as time and space are in constant movement.

Consequently, an assumption in Law is like, for example, the achievement of JUSTICE, it has different meanings and interpretations in distinct spaces and moments.

And as this manual does not claim to be just a work of philosophical theory, we will see, from a positivist perspective, what limits Law finds today that it can apply in the other world, or as we call it here: Cyber-space.

3.5.1 The Principle of Territoriality- Universal Justice?

The principle of territoriality can be defined as those criteria which establish the exclusive application of a law of a determined territory to all the events that were committed within it.

Namely, the principle by which the laws have "borders" which are traditionally limited to the terrain in which the power which has passed them governs.

It is the principle and most stand out limit of Law, for that we can affirm, from a global perspective and without being exhaustive, and in a concrete legal system, that the State has the power to legislate and apply laws within its physical borders; meaning, the territory that the State is comprised of and that encompasses, not just the land, but the territory's neighbouring seas and air.

That said, there is no doubt that this territorial principle is not absolute, meaning that there are exceptions. There are hosts of laws are regulations that reach beyond a single State. The famous International Agreements are a clear example of this.

But here what we want to highlight is that the theory applied from the principle of territoriality, commonly accepted by the doctrine, is not applicable in Cyber-space due to the obvious, and previously explained, reasons.

Cyber-space is not limited by physical borders and not even by cyber-borders. Any website with a URL address can be accessed from any device, and by definition, the location in one territory or another in the physical world does not determine whether or not this network can be accessed.

In this regard it can be argued that the are exceptions, for example the veto that the Chinese Government has put on certain foreign web pages, or the limitations that are in place on their own web pages so that they do not appear in certain countries. But these are Ad-Hoc exceptions and restrictions that have been put in place to avoid the internet's innate capacity to reject the borders that have traditionally existed.

Consequently, the separation of powers that took place during the French Revolution (legislative, judicial and executive powers) is not applicable in Cyber-space. Likewise, neither is the separation into "territories" of different governmental units.

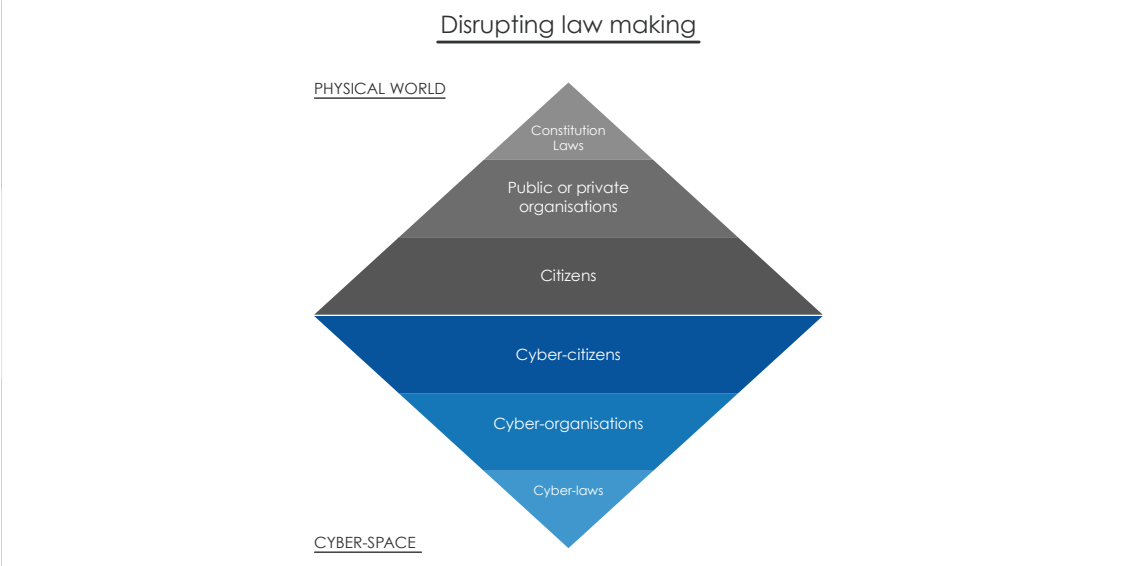
Although there are some small exceptions, there are a series of rules that are commonly accepted by internet users.

An example of that is the normative that regulates the assignation of domains and the resolving of conflicts that those assignations may provoke.

Likewise we see a whole range of bilateral contracts between e-commerce companies and the customers which aim to purchase their services or products. And what can be said about the general conditions or legal warnings (which are another example of the contract of adhesion) from key protagonists like Apple, Facebook, Amazon and Google?

But, leaving these exceptions to one side, on the internet there is not a legislative power that enacts laws which must be complied within each "territory" as there are not differentiated territories to regulate. Likewise, there is no legislative power (although technically speaking in this case it would not legislate, but order) that dictates the rules for all of cyber-space and all of its users in a complete and uniformed way.

This is the root of many of the problems that currently arise regarding the ordering of cyber-space, and it is one of the most vital and important points that will appear regarding the conception of Law within the coming chapters of this book.



3.6 A New Profession: the Cyber-lawyer

We have seen that in cyber-space, the States and their governments lack the legitimacy and democratic representation that we currently recognise.

However, true companies that have been born on the internet are emerging, as too are companies that exist in the physical world and make the most of cyber-space to launch their services and products. These companies located on the internet will be referred to as "cyber-companies".

The cyber-companies are a virtual representation of i) companies that are lawfully established in a State and those other ii) for-profit organisations that without being lawfully established, act on the internet; both have their own domain names.

Just as these cyber-companies exist, it is obvious to point out that the most recurring and important element in cyber-space is the individual or internet surfer. To put it better, the virtual representation of the individual, that we can call the "cyber-citizen".

This individual accesses the internet via a "border" and "customers" of an ISP or telecommunications company and by means of a hardware device that surfs the internet, becoming a cyber-citizen.

This cyber-citizen normally interacts on the net in a double faceted way, personal or professional and public.

And this last professional and public role is what I would like to highlight in terms of the legal profession.

What role does the lawyer have on the internet?

If Law can be described as the discipline which studies laws and their application, or how the group of rules, laws and principles order life within society, the lawyer has been configured as an essential agent within that society.

Its role in the world is fundamental when it comes to conflict resolution. And often, its preventative advice can even avoid future breaches. When the conflict already exists, its role in defence of a client is a basic element (the right to defence) of a state of Law.

And so, this agent of utmost importance in the earthly world suffers a true metamorphosis in the cyber-world.

To start, on the internet there is no kind of body that enables the lawyer, as we currently know it. However, it is a "reality" that in the next few years the so-called "virtual lawyers" will start to appear.

And I am not talking about lawyers specialised on the law of information technology, but rather lawyers that professionally practice on the net, offering intrinsically virtual services, such as, for example, the drawing up of forms, documents and contracts.

It should be pointed out how between 1990 and 2010, a new professional lawyer emerged, specialising in information and communication technology.

But I would go as far as to say that the technological revolution has even caused these professionals to have to adapt, in current times, to a new reality or technological era: the Internet of Things and cyber-crimes are examples of that.

The 20th Century Lawyer Vs. the 21st Century Lawyer

I would like to point out that, to as far as my knowledge, there is a new figure on the internet called the "cyber-lawyer" who has these new qualities:

- Advises their clients from cyberspace
- Knows the problems of the internet
- Knows the territorial laws of their location, but knows the regulations that try to order cyber-space even better
- Carries out two roles: one in their physical-time space, where they advise citizens, organisations and companies in matters of ICT (Information, Communication Technology); and the second,

where it advises cyber-citizens and cyber-companies in a new environment, with new paradigms, conflicts and regulations.

- Voluntarily adheres to basic ethical regulation, although there is no organism that enforces this.
- Helps to resolve antisocial behaviour with the aim of trying to achieve a civic, peaceful activity on the net.
- Carries out tasks without human intervention.
- Automates legal tasks that can be carried out by computing.

20th c. Lawyer	21st c. Lawyer	Cyber-lawyer
Starts to use new technology	Loves new technology	New technology is part of their workplace tools
Uses paid for databases	Uses the internet as a database	Surfs the internet and generates knowledge in the data bases
Has a web page	Uses Twitter and Linkedin	Enters social networks as a cyber-lawyer
Is not much differentiated from the competition (commercial, criminal, civil...)	Is differentiated as a lawyer specialised in ICT	Is hyper-specialised in the internet and its regulation. Reinvents a discipline
The close, physical, personalised treatment of the client is what is important.	The important thing is to be immediately in contact with the client.	The important thing is to be virtually close to the client
Has a profound subject knowledge	Is specialised in a subject	Is hyper-specialised in a new discipline
Advises clients and/or organisations	Advises clients and/or organisations	Advises cyber-clients and cyber-organisations
Sees the physical world as it is perceived to advise their client	Sees the internet from their physical location	Sees the physical world from cyber-space

3.7 On the Internet, Are There New Legal Assets To Protect or Regulate?

At this level, a question should be put forward whose answer conditions the way of ordering the antisocial behaviour that is committed in cyber-space.

And that question is: are there new legal assets to be regulated in cyber-space?

Or, on the contrary: are the legal assets in the real world the same as those in the virtual world?

In terms of legal assets to order, the following should be highlighted:

- Heritage
- Privacy
- Image rights
- Intimacy
- Intellectual works
- Brands and patents
- Life
- Money
- Etc.

Diverse local, regional, international and supranational bodies understand that the legal assets to be protected on the internet are the same as they are regulated in the territories that they belong in, be that regional, national or international territories.

In other words, these bodies have the idea that cyber-space can be regulated through territorial bodies that are legitimised by local regulations, or by supranational bodies that are legitimised by agreements that have been signed and ratified by a determined number of countries.

Other voices or trends uphold that this form of regulating cyber-space will lead to its failure due to the inefficiency of the "traditional and territorial" form of ordering chosen. This will face great territorial principle application problems in terms of the applicable jurisdiction and the appropriate court for the actions committed in a virtual world that lacks physical space.

In this way, initiatives can be highlighted such as a Constitution for the internet or the ever increasing, important and influential movement for a so-called "government of the internet" where the so-called stakeholders or groups of interest that advocate for new regulations and "virtual" rules to order cyber-space can meet.

In both cases, following one or the other, right now doubts occur about the regulation of new assets that escape to known Law because of their complexity and their ubiquity. These new assets include, for example: virtual money or "cyber-money" such as the bitcoin; the deletion of personal data or the right to be forgotten; the "cyber-will" or what happens when somebody passes away but they still have a virtual avatar on the internet.

With the birth of cyber-space, there are even assets that are regulated in the physical world which acquire new attributes which greatly complicate their ordering. Thus, for example, the privacy on social media or "cyber-privacy" and the protection of digital content or "cyber-copyright" can be highlighted.

And finally, the new legal assets born on the internet that are already regulated exclusively in cyberspace without having a correlation in the physical world, such as those regarding internet addresses or domains should also be underlined.

4 Key Antisocial Behaviour on the Internet

4.1 Cyber-crime

In way of a recap of the previously expressed ideas, and as an introduction to the content of the next chapter, we have said that the group of rules that govern a determined territory in a specified time is called a legal system. It has been defined as such for centuries and is currently applied in every State in the world.

Disciplines such as Criminal Law, Civil Law or Prosecution are applied, in one country or another, on the basis of that definition. For example, Spanish Criminal Law is solely applied within Spanish territory, comprised of land, sea and air.
This basic principle of law is called the principle of territoriality and it implicates that every citizen knows that when they travel to a country and put their feet on that soil, they are subject to the laws of said country.

However, it turns out that cyber-space is a "territory" that lacks a physical space (not time), breaking all of the laws of nature that have been studied in theoretical physics (Einstein, Newton) and quantum physics (Richard Feynman). This provokes diverse and complicated equations to this other science and inexact discipline that is Law, whose model sees itself as threatened by this new social cyber-reality.

This means that the traditional criteria for classifying within a specific space cannot be applied to cyberspace and, for this reason, it is not possible to determine the rules that need to be applied and how they should be administrated in the same way as with a physical territory.

The same can be said for the case of cyber-crimes: The internet is made up in such a way that cyber-criminals can easily and cheaply carry out their antisocial actions anonymously by using a device (smartphone, computer etc.) that is difficult to territorially locate in the physical world.

The following question should be raised: if the cyber-criminal is found, but it is not possible to identify the physical place that he/she operates from, but that it "virtually located" on the internet, can that person be prosecuted?

The answer forms part of one of the key questions of cyber-law. Applying the rules of physical territories, those that carry out cyber-crimes cannot be prosecuted or convicted without incurring an excess of the powers of every legal system. But these same cyber-crimes cannot go unpunished and their perpetrators need to be prosecuted.

For this reason, the legal systems and cyber-organisations that face the problems that arise in cyberspace should reconsider the traditional legal point of view at look at cyber-problems from a new perspective, from the perspective of Cyber-law.

TERRITORIAL		CYBER-SPACE	
Who?	To be identified	Who?	
Where?	Place where it takes place	Where?	¿?
Applicable law?	Place where it takes place	Applicable law?	¿?
Appropriate court?	Place where it takes place	Appropriate court?	¿?
Territorial justice		Cyber-justice?	

4.2 Child Pornography

Child pornography can be defined as the group of activities through which economic gains are made by means of the explicit audiovisual representation of minors involved in sexual conduct, this may be real or simulated. It can also be said that this has become one of the most reprehensible and antisocial behaviours that is produced via the web.

4.2.1.1 Scenario

Audiovisual material, of any nature, which shows minors, regardless of their gender, in any kind of sexually explicit or merely erotic way can be considered as child pornography.

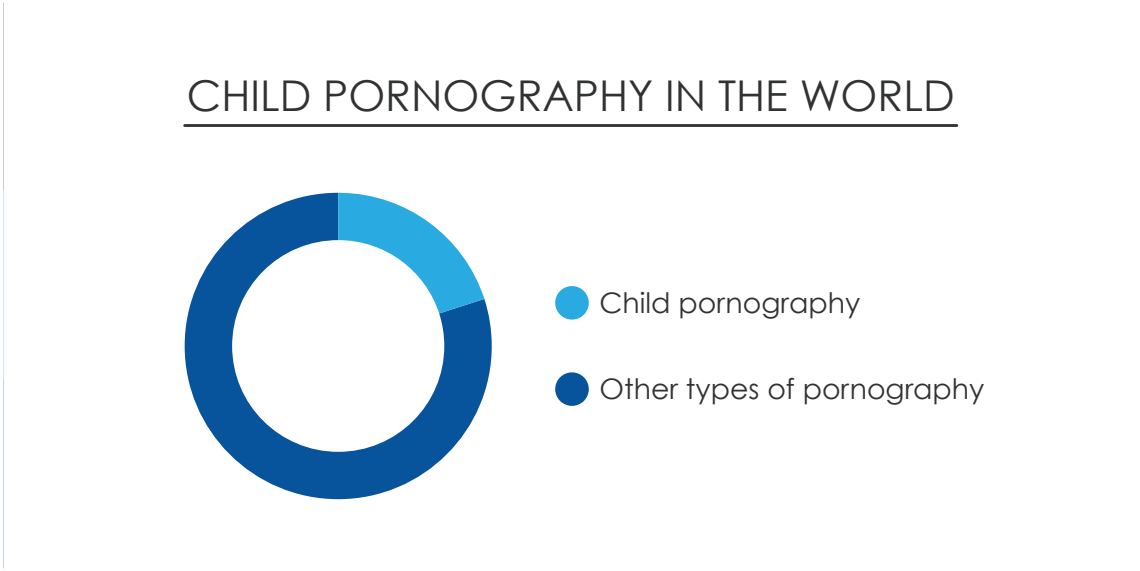
The crimes regarding child pornography include, in the legislation of every territory, the simple possession of this type of material, as well as its **distribution**, **exhibition** and the sharing of it with other people. Depending on the regulations, tougher prison sentences can also be enforced if the perpetrator is a blood relative of the victim.

On the internet, just like in the territorial world, cyber-pornography is the existence of this audiovisual material which portrays minors in sexual attitudes or poses. Due to the fact that the format that this material is contained in is irrelevant in terms of its consideration as pornography, it can be found in various ways in cyber-space: audio files, photos, videos etc., which are hosted and circulated on the internet.

Traditionally, many territorial legal systems punished the cyber-crime of child pornography as a standard child pornography offence. However, it is starting to become more common for territorial legal systems to establish longer prison sentences for those crimes regarding child pornography that are committed in cyber-space.

Since 1999 the number of cases of child pornography that have been reported have basically doubled, and this increase can easily be linked to the commercialisation of internet services in western countries.

Some international observatories, such as the National Centre for Missing & Exploited Children (NCMEC), estimated that of all the pornography on-line, around 20% can be classed as child pornography.



In this regard, Najat M'Jid Maala, a member of the UN, in one of her speeches voiced that some 750 thousand paedophiles are permanently connected to the web, where there are around 4 million websites dedicated to the content of child pornography.

4.2.1.2 Analysis

From the perspective of the territorial rules that the crime of child pornography is found within, diverse and heterogeneous regulations can found, but these crimes are always criminally punished.

In Spain this is regulated within section 189 of the Criminal Code, in which those that capture or use minors to carry out pornographic exploits or to elaborate the material that they contain, will be convicted of between 1-5 years in prison. Those that finance these activities, or make a profit out of them are also punished. The same sentence is applied to the selling, distributing and displaying of pornographic material. What is also now punishable, and this is relatively new compared to other legislation, is the mere possession or simple access to said material. The foreseen sentence in these cases is reduced to between 3 months and 1 year of prison.

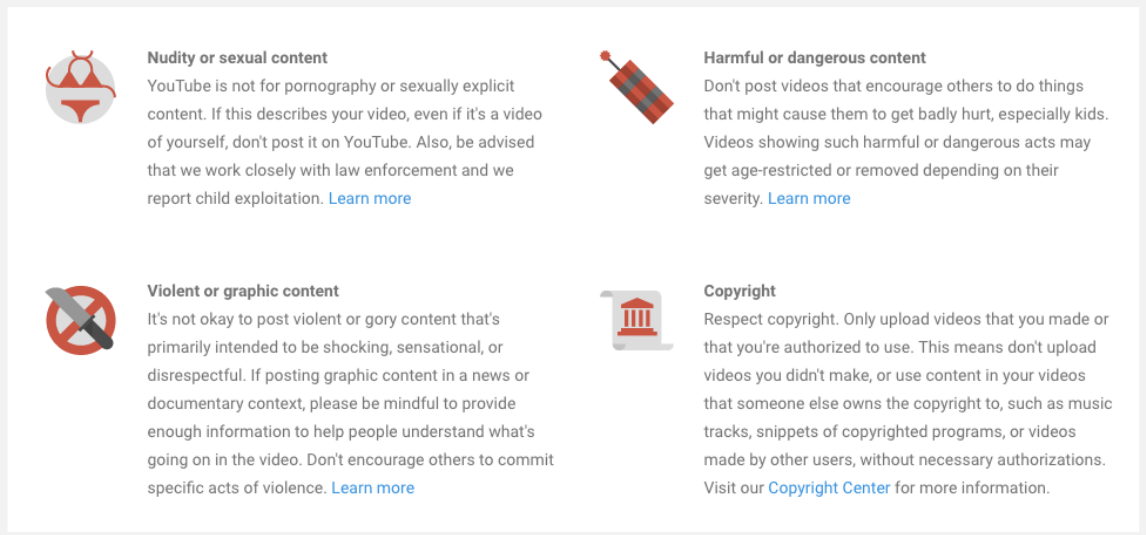
Some countries, such as the **Dominican Republic**, have opted for a new form of territorially fighting against child pornography in cyberspace: by creating specific legislation against the crime committed by means of information technology, as an additional criteria. In 2007, the Law No. 53-07 on Crimes and Delinquencies of High Technology was passed, this is complimentary to the territorial regulations against the commission of child pornography crimes in the country. The protection is articulated in the following way:

- In the Code for the Protection of Children and Adolescents, it is established that the physical or legal persons that produce or elaborate audiovisual material

(photographs, videos or other publications) where minors are represented, will be convicted with prison sentences of between 2-4 years.

- The Law on Crimes and Delinquencies of High Technology punishes those that produce, spread, sell or commercialise child pornography by means of information technology with prison sentences of between 2 and 4 years, whilst the possession of said material is punishable with sentences of between 3 months and a year.

Regarding the ordering carried out by the cyber-organisations on the internet themselves, the **YouTube** Community Rules, to use an example, do not allow the publishing of any type of pornographic or sexually explicit content. The publication of videos that contains sexual material where minors appear is prohibited, as is making a simple comment. Should it find such material, YouTube blocks the perpetrator's account and it reserves the right to report this to the appropriate territorial authorities, it also collaborates with them to prosecute the crime.



Nudity or sexual content
YouTube is not for pornography or sexually explicit content. If this describes your video, even if it's a video of yourself, don't post it on YouTube. Also, be advised that we work closely with law enforcement and we report child exploitation. Learn more

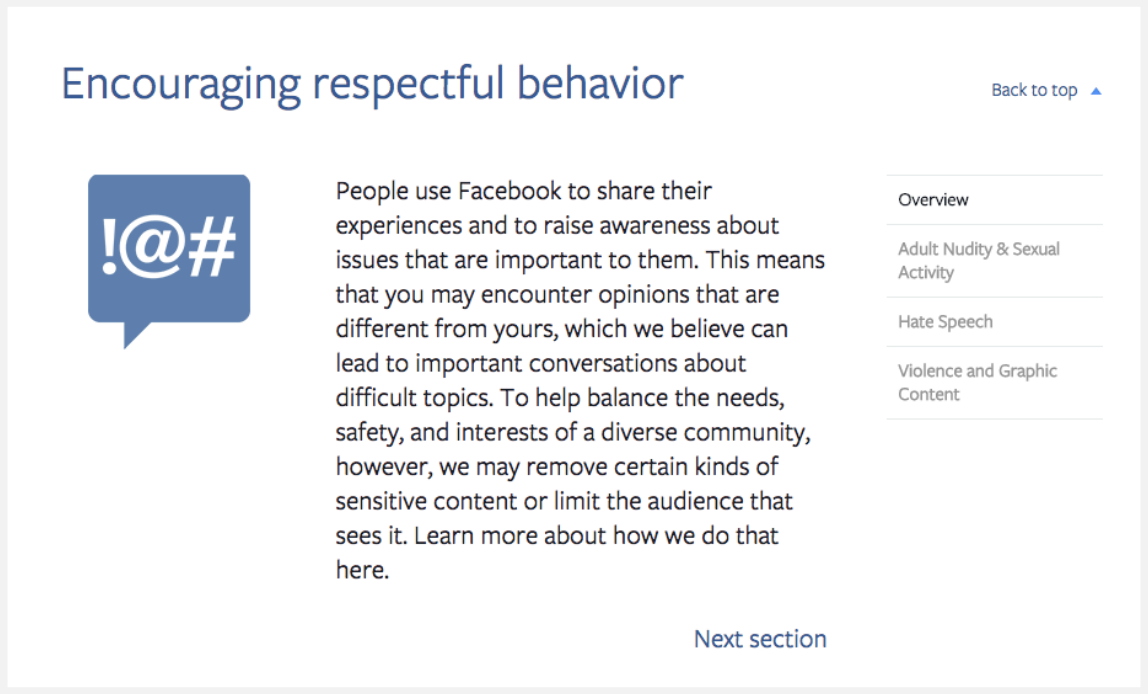
Harmful or dangerous content
Don't post videos that encourage others to do things that might cause them to get badly hurt, especially kids. Videos showing such harmful or dangerous acts may get age-restricted or removed depending on their severity. Learn more

Violent or graphic content
It's not okay to post violent or gory content that's primarily intended to be shocking, sensational, or disrespectful. If posting graphic content in a news or documentary context, please be mindful to provide enough information to help people understand what's going on in the video. Don't encourage others to commit specific acts of violence. Learn more

Copyright
Respect copyright. Only upload videos that you made or that you're authorized to use. This means don't upload videos you didn't make, or use content in your videos that someone else owns the copyright to, such as music tracks, snippets of copyrighted programs, or videos made by other users, without necessary authorizations. Visit our Copyright Center for more information.

Example of Youtube's Terms and Conditions
Source: https://www.youtube.com/yt/policyandsafety/en/communityguidelines.html

Facebook establishes some conditions that should be accepted as a whole so that users can use their service. These conditions, known as "Facebook's Statement of Rights and Responsibilities" establishes that:



Example of Facebook's Terms and Conditions.
Source: https://www.facebook.com/communitystandards

- The publication of any kind of pornographic content is prohibited.
- It is prohibited to use Facebook for illicit acts.
- The exchange of material that may be considered as child pornography, including naked minors is prohibited.

Not complying with these rules can lead to a total or partial blocking of the user's account, regardless or not of whether the social media itself decides to report the illegal act to the appropriate territorial authorities.

Another example to take into account could be that of **Instagram**. In their Conditions of Use, the content that users can upload to its servers is limited, uploads of total or partial nudity are prohibited, and additionally the explicit posting of pornography or sexually suggestive photos is also prohibited. Minors are not expressly mentioned, but it can be understood that they are included within these rules.

4.2.1.3 Proposed Solutions

It seems as though there is not a great discussion in terms of considering any type of child pornography as unacceptable, in the good use of the internet.

To avoid the circulation of this type of content, the approval of an identification protocol "ID Protocol" embedded within the TCP/IP protocol (which will be later described) must be championed.

There should also be the championing of the approval of cyber-rules that impose cyber-restrictions, such as, for example, the cancellation or suspension of an account; in other words, not allowing free surfing to a certain type of cyber-citizen. These initiatives are

being carried out on an individual basis, as has been seen previously with the key cyber-organisations. But in what is known as the "Deep Web", this does not happen.

States should make an effort to, in a collective and majority way, pass national and supranational regulations that include sanctions that combine sentences of the restriction of freedom (prison) with cyber-sanctions of the restriction of surfing (cyber-prison) or cyber-solutions, understood as the impossibility for a citizen to use the internet and networks depending on a specific location within a State.

Meaning that, together with the term of imprisonment, they should be convicted to not being able to access the internet through any ISP located within the State's territory or borders during a set period.

An example to follow, and this kind of conviction is becoming more common, is the famous ruling in June 2015 in the Provincial Court of Barcelona in which a 25 year old was convicted of 4 years in prison, to economically compensate their victims and to not use social media, nor chats, nor Whatsapp for 5 years as a conviction of crimes regarding sexual abuse and child pornography.

4.3 Cyber-Advocacy of Violence

Due to the wide extension of social media in the current cyber environment, and the freedom and lawlessness that the internet grants its users through easy anonymity, one of the behaviours that have grown the most in recent years is the cyber-advocacy of violence.

4.3.1.1 Scenario

The advocacy or glorification of terrorism and violence is the discourse or declaration in favour of criminal acts of violence, commending and defending so as to justify their use in certain situations and, indirectly promoting actions related to this phenomenon.

For the purpose of this book, both terrorism and violence must be understood in the widest sense possible, taking into account all kinds of illegal, violent, offensive, abusive, defamatory, harassing or incorrect behaviour.

For practical purposes this is about a behaviour that is very much pursued by the key international organisations. A test to that, as an example, is the UN Security Council's Counter Terrorism Committee's yearly Summit against Terrorism, which was last held in Madrid, Spain, in mid-2015. And together with that there is a wealth more of meetings and conferences that focus exclusively on the eradication of this problem.

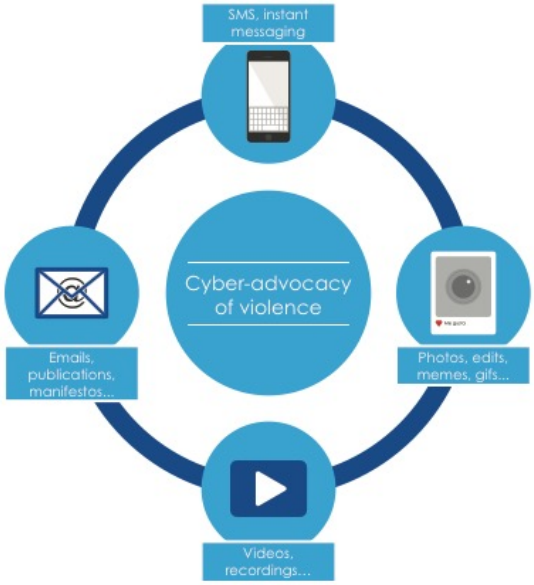
On the internet, the advocacy or cyber-advocacy of violence has the same definition, but expressed via the web , which, due to its large transmission, is converted into the main channel of communication for those that carry this out.

Cyber-advocacy is seen more and has a higher incidence rate on social media, such as on Twitter or Facebook, where messages can be sent with more ease and virality. However,

this type of behaviour also tends to happen on thematic forums or blogs, such as those that belong to the platform Blogger, and on video sharing platforms such as Youtube.

Example of cyber-advocacy of violence on Twitter: Source: twitter.com

The way the message is communicated can be done in many different ways, such as via the written word, images, videos and recordings etc. Every medium that is able to be transmitted on the internet can be used to commit a cyber-advocacy of violence.



Those subjects that can realise this behaviour can do so in an individual or group basis, forming pressure and mobilisation groups. It is also possible for cyber-advocacy to be carried out in a covert way by individuals under the address of an organisation or company, with the aim of influencing the market where they operate against their competition.

The victims of this behaviour can vary in terms of their circumstances and a multitude of factors. The cyber-advocacy of violence can be directed towards an individual or group, a company or collective organisation and even to institutions and bodies that form part of the State.

The key elements of this behaviour are:

- They promote violent acts
- The humiliation and despise of their victims
- Interest in the largest possible spreading of the message: virality

DAILY NEWS 27/08/15

The murder of two reporters in a town in Virginia, on the east coast of the United States, at the hands on an ex-employee of a news channel has turned the world upside down in these last few hours due to the virality that has reached after the murderer posted the video of the crime on social media.

On Wednesday morning, Vester Lee Flanigan, known by his stage name Bryce Williams, shot two ex co-workers from the local news channel that he had worked at as a presenter. The local authorities reported that he later died from self-inflicted wounds. However, in comparison to other gun-related murders in this country, this act has been very controversial for various reasons which are directly related to the media.

The crime was committed in the first place whilst the victims, interviewer and cameraman, filmed a live report for the channel. Therefore, the crime was screened live on the television without censoring to all the televisions across the United States that were tuned in to the news channel.

Following that, videos that William's had filmed from his mobile phone appeared on his Twitter account, as well as tweets which accused the victims of professional arguments which had apparently happened

in the past at the channel and he questioned the racism and professionalism of his recently murdered co-workers.

Finally, it seems that the ABC News station also received a more than 20 page document from Williams two hours after the shooting, in which he justified his actions and praised himself for killing his ex co-workers. They also received a call in these period of time in which the murderer confirmed his identity and took responsibility for his actions.

According to the information on the channel's website, Williams had been calling ABC during the past weeks, saying that he wanted to launch a story (he did not specify which) and he wanted to fax the information to them.

Leaving the motives that led the perpetrator to commit this crime to one side, what is striking is William's need to upload his video to social media, to cyber-advocate the violence via Twitter and Facebook and to make his actions renowned. The information uploaded by ABC gives off the impression that he wanted to make his story go viral and to spread his message of hate and violence, and that is exactly what is happening.
His Twitter and Facebook profiles have been blocked and the videos have been deleted by the administrators of both companies, but that has not stopped them going around the world.

There have been other occasions in which these organisations, as well as Youtube and other video storing platforms, have been able to censure the immediate contents, locating and identifying the author, leading to his arrest. But this was when the videos uploaded stated the intentions of committing a crime before actually doing so, in this case however, virality was achieved, but the events happened in reverse order.

4.3.1.2 Analysis

The treatment of cyber-advocacy of violence is distinct according to the location and environment where it happens, furthermore it will also depend on elements such as the socio-political environment and the armed or violent conflicts that can affect the territory that creates or changes its laws.

For example, after the attacks in Paris this autumn by the radical Islamic group DAESH, it is very probable that measures will be approved so as to limit the advocacy of violence in this country in a stricter fashion, (that is what the predictions state) than in other European areas which have not had up-close experience of violence for a reasonably long time.

In the majority of States, advocacy of violence is considered as a crime and is included within each country's distinct Criminal Codes, despite the differences in other political, or even legal, fields. The sentences tend to be less than a year's imprisonment, or a small economic sanction. There is not one case which refers to its expression by means of ICT or telecommunications. However, its realm of application is not restrictive and cyber-advocacy can be included within these behaviours.

For example, in **France**, at the moment this behaviour is included within section 431.6 of their Criminal Code which states that: "Any person that incites an illegal armed meeting by means of shouting, public speeches or by means of disclosed or distributed written means, will be punished with one years' imprisonment and a 15,000 euro fine"

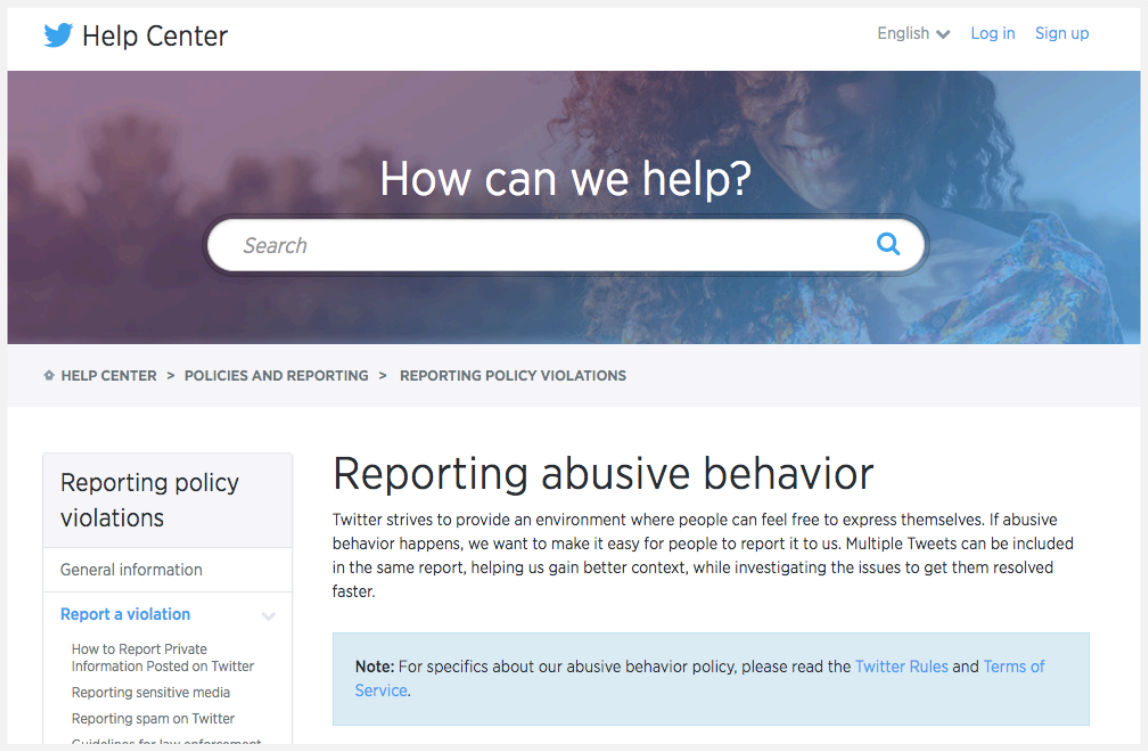
The State of **California, U.S.A.**, punishes these types of actions with sentences which are equally less that 1 year of prison or a less than 5,000 dollar fine, as stated in section 422.6 of their Penal Code.

Even **Costa Rica** establishes in **section 276** of their Criminal Code that**:** "Any persons sentenced for a crime, or who publicly advocates a crime, will be restrained with a prison sentence of between 1 month to 1 year or with 10 to 60 days' fines".

In terms of the ordering that the cyber-organisations within cyber-space carry out, it is usual practice for there to be a clause within all of their Terms and Conditions which prohibits users from promoting illegal activities or other acts of violence in general:

For example, on **Twitter,** the Terms and Conditions and the Rules of Use prohibit the following:

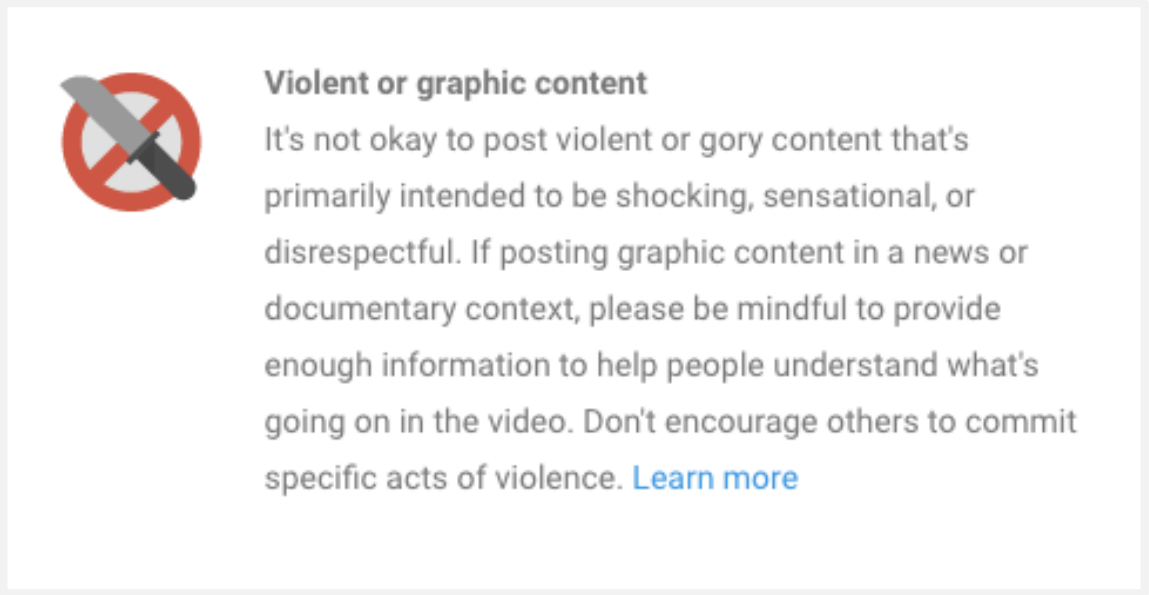
- Publishing or sending direct threats or specific threats of violence against others.
- Using the service for any illegal aims or for the promotion of illegal activities.
- Participating in abusive or harassing behaviour directed towards other people.



Example of Twitter's help centre.
Source: https://support.twitter.com

On **Wordpress** the management of the blog is the responsibility of the collaborators and it is established that: "If you operate a blog, comment on a blog, post material to the website, post links on the website, or otherwise make (or allow any third party to make) material available [...] you are entirely responsible for the content of, and any harm resulting from, that Content. That is the case regardless of what form the content takes, which includes, but is not limited to text, photo, video, audio, or software. By making content available to the public, this represents and guarantees that:

- The content is not pornographic, it does not contain threats or provokes violence; likewise it does not infringe privacy laws or thirds person copyright laws.



Example of Youtube's Terms and Conditions. Source: https://www.youtube.com/yt/policyandsafety/en/communityguidelines.html

Another example is that of **Youtube,** which states in its Terms and Conditions, regarding behaviour linked to the cyber-advocacy of violence, that:

1) Content is not permitted which promotes or consents to violence against individuals or groups for reason of:

- Race or ethnic origin
- Religion
- Disability
- Gender
- Age
- Nationality
- Being a war veteran
- Sexual orientation
- Gender identity
- With the aim being to incite hate for one of these reasons.

4.3.1.3 Proposed Solutions

All proposals for the legal ordering of cyber-acts of advocacy of violence should be understood in depth and case-by-case, as in all advanced and democratic countries there is an invaluable legal asset of freedom of speech, which is one of the fundamental pillars of a developed country.

However, in the most transcendent cases, such as Islamic State's (DAESH) recruitment and spreading of violent messages, it seems that the proposal for legal ordering should be carried out from the perspective of other connected perspectives.

From the personal and domestic fields, the cyber-advocacy of violence should be ordered from a focus on protection or security of the private field, in combination with the protection that is offered from the public field. This means that it seems to be important that when somebody is the subject of a case of cyber-advocacy of violence, they should protect themselves with private security controls such as the blocking of the user's accounts, physical measures of self-protection, self-surveillance and content control in terms of all the blogs or web pages relating to the person.

Likewise, this "victim" of cyber-violence should make the appropriate authorities aware, so that said State can take the appropriate measures to protect the person.

In the realm of cyber-organisations, the solution proposed should contain self-security control objectives (self-regulation of their content) coordinated with the appropriate public authorities.

A test of the power that these networks hold in the popularisation of this behaviour is the, previously mentioned, most recent UN. summit, where conclusions were drawn regarding the European and global strategies in the fight against this problem. Said conclusions were that is vital to **highlight the importance of the implication of companies that manage social media, such as Facebook, Google and Twitter, in the fight against terrorism.**

Without specifying concrete measures, the U.N. mentioned amongst its closest possibilities, working with the private sector, with cyber-organisations like Facebook, Google or Twitter, to apply surveillance measures to its networks, and so that when they find evidence, it would be possible for justice to be done and for those people that recruit terrorists on the internet to be sentenced. They also advocate working to actively eliminate the radical content available to the public, as well as including messages that counter this content.

At a State level, it seems that the solution proposal will be aimed at the collaboration between diverse countries and at the creation of cyber-bodies of cyber-police and cyber-military that monitor and protect cyber-space.

This, logically, will bring with it the arrival of appropriate regulations or laws, and above all the enabling of cyber-capabilities of the staff that will carry out these new technological skills.

From my point of view, very soon we will see how these public security cyber-bodies start to be created.

4.4 Industrial Cyber-espionage

Espionage has and will always exist, but the massive spying on citizens and companies was a reality that was unknown by the majority of people.

It seems as though NSA (National Security Agency) has collected a mass of information in recent years using the "back doors" of the servers of great operators of the internet industry like Google and Yahoo.

This massive collection of data can be defined as a clear example of Big Data. But what can we understand as Big Data in this current case? And even more importantly, is the processing of this data legal? What legal conflicts arise from now on?

This present case draws a clear example of electronic surveillance or cyber-espionage within the NSA. They have used complex information systems to capture, store, process and analyse immense quantities of data. We could call this "**Big Data Brother**"**.**

The NSA has stared in one of the biggest cyber-espionage scandals in history.
Source: https://es.wikipedia.org/wiki/Agencia_de_Seguridad_Nacional

Against the publication of that alarming news is the European Union, governed by diverse political leaders that cannot or do not want to make the most of the situation, at least, to defend the rights of their European citizens. An example of that is the delay that has taken place with the passing of the European Data Protection Regulation.

To this stand-out international conflict, the underlying legal conflict must also be added in the collision of the so-called privacy and/or intimacy rights before the protection of citizens by States or national security.

Governments are well within their rights to protect their citizens against any organised criminal attack, but, is it legal to do so outside of their physical borders? Can they collect the personal information of citizens and companies from around the world? And moreover, is there a proportionality between the pursued, the security and national defence, and in terms of the fundamental rights and freedoms of foreign citizens?

It should be highlighted that industrial espionage had been happening illegally, but what lawful governments were doing was unknown. With this information being true, it could be thought that said activity was bring American companies certain competitive advantages compared with leading European companies, for example in the public tendering of large infrastructure.

And in terms of the cyber-espionage of citizens, the supposed violation of the personal privacy and intimacy of foreign citizens that do not allow the electronic handling of their personal data with unknown aims should be noted

4.4.1.1 Scenario

Industrial espionage can be defined as the activity of covertly obtaining information, communications and data of third parties, of a an industrial or commercial nature and which is not available for the public's general knowledge, using techniques such as the infiltration in faraway organisations, data robbing, bribery or blackmail.

On the internet, this type of cyber-espionage consists of the same searching for the obtaining of information and data, but using the technology available via the internet as a means of access the information and communications that circulate the web or that are stored in information or technological mediums.

The data that is tried to be obtained most often is that regarding intellectual and industrial property, patents and financial or economic data from companies or industries.

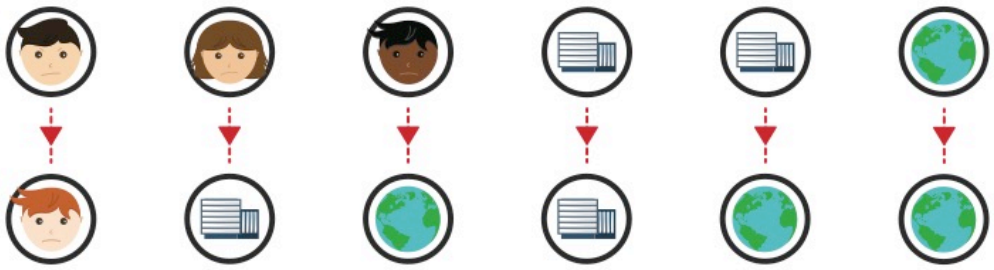
Industrial cyber-espionage is when the data from (non-military) companies and organisations is pursued, whilst if it is personal data being pursued it is referred to as access to content without permission.

The mediums that can be used to carry out this conduct are not uniquely limited to personal computers. Cyber-espionage can happen on tablets, smart phones, storage devices or technological equipment of another nature. Every system or medium with the capacity for the entrance and exit of data is susceptible to spying, such as for example the personal information of a director working from home.

In this regard, the types of cyber-espionage that can be produced in accordance with those affected or involved are:

- **Individual-Individual:** A cyber-user obtains information and personal data, normally from another employee of a large company or corporation, via their person computer, smart phone or tablet.
- **Individual-Organisation:** A cyber-user obtains data and information about an organisation directly via their information systems.
- **Organisation-Organisation:** An organisation obtains information and data from another organisation, normally a competitor, in order to gain a competitive advantage.
- **Organisation- State:** An organisation seeks to gain information from the different organisations that the State is divided into (Ministries, Agencies etc.).

- **State-State:** A state obtains information and data from another for the benefit of the organisations that make up that State, or for National Security reasons.
- **State-Individual:** A State gets an individual's information and personal data; once again this can be via their personal computer, smart phone or tablet, as well as through the different official registers and mechanisms.



4.4.1.2 Analysis

Cyber-espionage is considered in very different ways in the internal rules of different organisations before the regulations that are gathered in the laws of different States, where there are also noticeable differences.

In this sense, it should be highlighted that there is a clear difference between the States that have regulated particular laws for these cyber-conducts and those that have simply added factual situations to the behaviours that were already dealt with in their laws or codes.

Venezuela is within this first group, with a Special Law against Computer-Related Crime (30 October 2001 Official Gazette No. 37.313) which classifies cyber-espionage as the "Violation of data or information privacy of a personal nature." And in Section 20 it establishes a prison sentence of 2 to 6 years and a fine of 200 to 600 tax units.

However, other States such as **China** consider these types of crimes within the Criminal Code. Sections 110 and 111 state that anyone who steals, meets in secret, buys or illegal offers State secrets or intelligence to a foreign organisation, institution or person will be punished with minimum prison sentences of 5 years, with a maximum of 10 years. However, in more serious situations, minimum sentences of 10 years can be imposed, together with other measures such as the deprivation of political rights.

Germany, in this case, also has sections within its Criminal Code that contemplate less severe punishments. For example, section 204 of the German Criminal Code punishes those that illicitly exploit a business or commercial secret to a third party with a prison sentence of up to 2 years in prison or a simple fine.

The more than evident differences in sentences among different territories, as can be seen in this small selection, is a reflection of the circumstances in each State which condition the treatment of this behaviour, with it being considered as a serious crime against the State in some cases, and in other cases a simple crime against industrial property or a computer related crime etc..

Since consistency cannot be found regarding the treatment of these crimes, one must deal with what each territory establishes in order to gain an answer to the degree of seriousness that is attributed to this behaviour in each place.

For the regulation in **cyber-world**, treatment, in change, is carried out in an almost identical way in each of the organisations that are subject to analysis from a cyber-law perspective.

For example, the leading organisation in video storage, **Youtube,** establishes within its Terms and Conditions regarding cyber-espionage that:

- Users are prohibited from collecting the personal data of other users from the Web Site or the Services.
- Accessing the content by any other technology other than the video playing web page or other available means is prohibited.

In the case of **Alibaba**, and its affiliate company **Aliexpress**, the example is similar and their Terms and Conditions that it is prohibited to do the following:

- Copy or reproduce services or any information, text, image, graphic, video, sound, directory, file, database or list etc. that is available through Aliexpress.
- Collect content from the site to create lists, databases or directories.
- Make use of any content for any aim that is not expressly permitted within the Terms and Conditions.

And to finish this series of examples, another example of this homogeneity could be the rules of **Facebook** which establish that:

- The user cannot collect information or content from others users nor can they access Facebook by using automatic means (such as harvesting bots, robots, spiders or scrapers).
- The user cannot request sign-in information or access the account that belongs to another user.
- The user cannot use Facebook to commit criminal, deceitful, malicious or discriminatory acts.

The majority of cyber-organisations, such as those mentioned in the previous examples, prohibit, to a greater or lesser extent, the unauthorised use of their platforms and the unauthorised obtaining of data. This reveals that cyber-espionage is a wide-spread conduct that is taken into account when clearly prohibited and specifying certain user behaviours.

A clear example of industrial cyber-espionage could aim to get the Coca-Cola formula.
Source: https://pixabay.com/en/coca-cola-can-cola-coca-drink-862689/

4.4.1.3 Proposed solutions

As far as I am aware, the secret to resolving this cyber-behaviour could lie in the proportionality and fulfilment or compliance of an international regulation.

It seems disproportionate to have to "frisk" through the personal information of millions of people to be able to predict and stop a crime before it happens.
If we do not want to create social alarm or have the legitimate representatives of the citizens violate the infinity of their fundamental rights, we should regulate said activity and inform the citizens, and surely the vast majority would understand.

It is within the State's rights to protect their territories. The aim that they pursue is commendable (defending themselves from organised criminal attacks) and surely other States will indirectly benefit from this. However, these activities regarding the computer processing of data should adhere to the known democratic channels, such as the international consensus, passing and disclosure of the relevant regulations.

In terms of the organisations, based on the fact that the gaps in security are, on the whole, due to the organisation's internal personnel, the solution proposals need to be directed at carrying out technical and procedural controls that minimise the risks of data leakages of internal information or those that can be accessed externally.

To do this, it is recommendable to follow international standards such as the ISO 27000-Information Security Management Systems- in a company basing itself on the following objectives, which, if fulfilled can guarantee a correct limitation of cyber-espionage:

1. Preserving information in such a way that it cannot be accidentally or intentionally deleted or lost.

2. Maintaining the confidentiality of information in such a way that third parties cannot access it without authorisation.
3. Making the information available in such a way that its access is not altered or prevented.

4.5 Cyber-harassment

Bullying is the behaviour that involves consistently pursuing somebody in a persistent and annoying way, provoking a situation of distress, emotional blockage and/or worry. This behaviour may go alongside acts of verbal or physical violence, threats, intimidation, extortion etc.

When this behaviour takes place on the internet it is known as cyber-harassment or virtual or cybernetic bullying . It consists in the victimisation, humiliation or any other type of annoyance regardless of the electronic device that is used: Smart phone, tablet, computer, wearable devices etc.

A determining element for it to be considered as harassment and not another type of cyber-behaviour is the time period of these actions. Only actions that take place during a continued and prolonged period of time, in a progressive way, can be considered as harassment, not those one-off or circumstantial actions that take place in a given moment. **It is also important to note that it can come to be small acts of constant violence that are very harmful and that, in the long term, can cause irreversible consequences to the victims.**

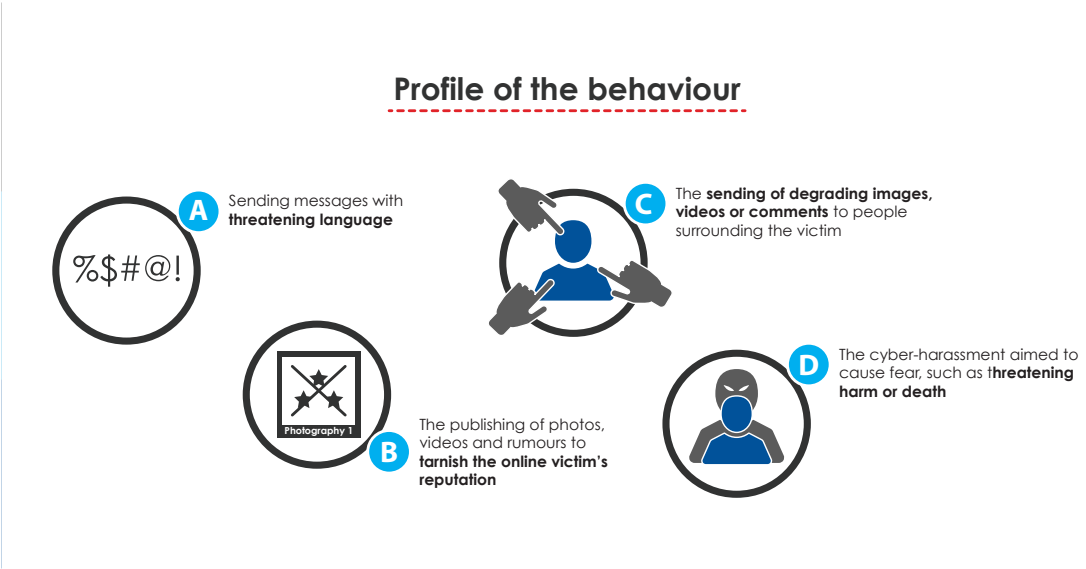
There are many ways of classifying cyber-harassment, such as, for example, the field or context in which it occurs:

- Schoolcyber-harassment: The psychological or verbal abuse which happens among minors.
- Professional cyber-bullying (mobbing): The ensemble of harassing actions in a working environment which causes the worker to feel fear, disdain and discouragement.
- Psychological cyber-harassment: The degrading and discrediting treatment of a person with the aim of making them psychologically unstable.
- Sexual cyber-harassment: The manifestation of a series of compulsive behaviour requesting unsolicited sexual favours.

Given its definition and the varieties that it can come in, cyber-harassment can be seen in the following examples:

- Registering the victim on a website which votes for the ugliest, least intelligent or fattest person with the aim of it receive the most votes.
- Creating a fake profile, impersonating the victim's identity, on social media or forums and publishing, in the first person, sensitive information regarding confessions such as certain personal events or explicit demands for sexual relations.

- Publishing information, images or offensive images on any internet platform which will infiltrate the victim's close environment and harm their dignity.



4.5.1.1 Analysis

In terms of countries and organisations, the regulations regarding this behaviour are heterogeneous and, above all, very scarce due to the fact that cyber-harassment tends to be included amongst the regulations of other conducts such as threats, extortion or advocacy of violence in a physical regard, under which the cyber version can be included. However, the regulation of this cyber-behaviour in a school and educational environment is starting to extend due to the devastating consequences that this type of bullying has on children and teenagers.

As indicated above, there is very little legislation that includes harassment as a separate behaviour. One example of this is the **Spanish** Criminal Code, which in section 172 ter, states that any person who harasses another in an insisted and reiterated way, without legal authorisation, by carrying out one of the following conducts, and therefore seriously disturbing the development of their daily life will be subject to between three months and two years in prison:

- Watching, pursuing or searching to be physically close to the other person.
- Establishing, or trying to establish contact with the other person through any means of communication or through third parties.
- Acquiring products or merchandise or contracting services through the wrongful use of the personal data, or making third parties get into contact with them.
- Impinging on the freedom or estate of the other person, or on the freedom or estate of people close to them.

For their part, some North American States now consider cyber-harassment within their sectoral regulations (within education, for example. One of those is the State of Tennessee (Tenn. Code Ann. § 49-6-1014) which expressly mentions cyber-bullying, what is meant

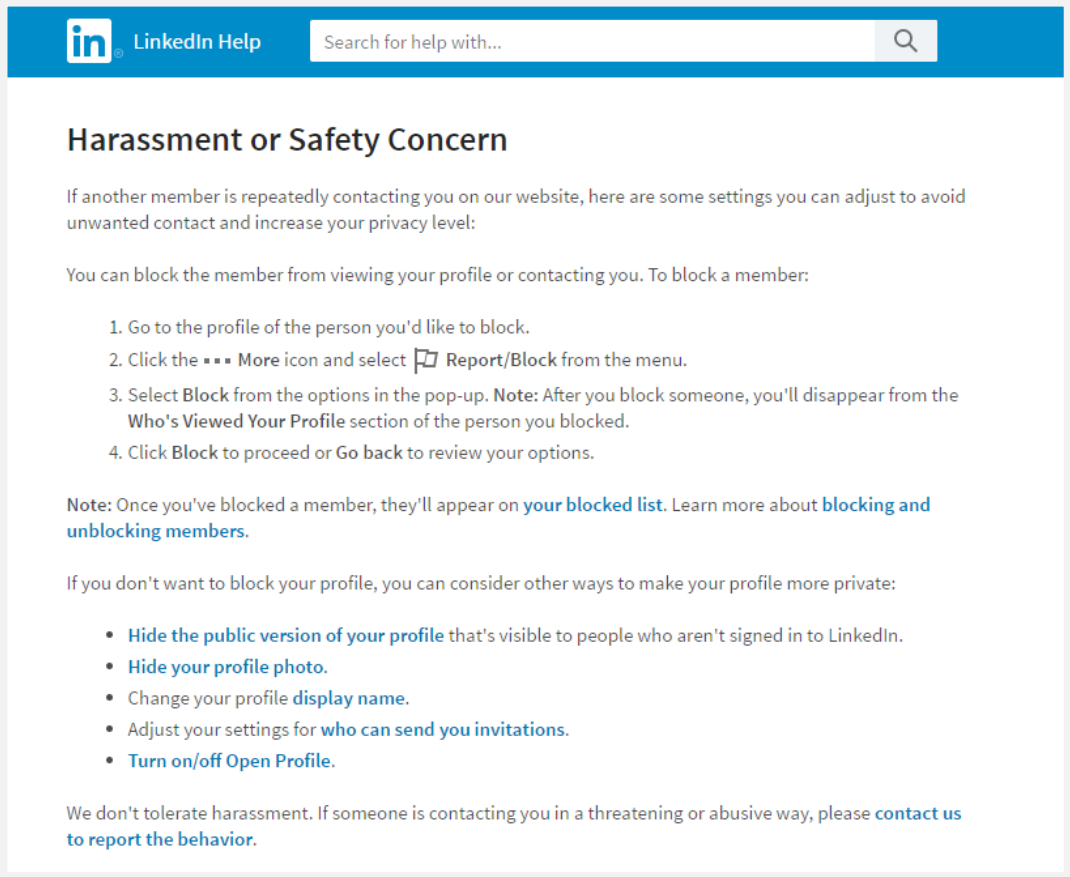
by online harassment, the means by which it can be committed and the corresponding sanction if the act were to be committed.

In terms of regulation of said conduct in cyber-space, a parallelism can be found with the current situation in the physical world, with some organisations that specifically mention cyber-harassment within their policies, and others that only make reference to and prohibit the expression of such on the web.

A clear example of the first type of organisation is **Yahoo**, which includes within its Terms and Conditions that users should not do anything with Yahoo Services, and they should not send other users content that is:

- Obscene
- Threatening or violent
- Insulting or damaging to others (even for minors)
- Invading the privacy of others
- Encouraging hate
- Encouraging bullying
- Encouraging discrimination or that is unacceptable for any other reason

Linkedin, also considers this behaviour within its Terms and Conditions of use, providing its users with a complaint form in the case of persistent, abusive behaviour:



Example of LinkedIn's Help Centre.
Source: https://www.linkedin.com/help/linkedin/answer/43781?lang=en

On the other hand, Ebay establishes, by means of its Terms and Conditions, that they reserve the right to cancel the services and accounts of users if:

- "we consider that you are creating legal problems or possible legal responsibilities,
- we consider that said restrictions will improve the security of the Ebay community or they will reduce the exposure to economic responsibilities, both for Ebay and for the users;
- we consider that you and infringing third-party rights;
- we consider that you are acting in such a way that is incompatible with the agreement or spirit of these Conditions of Use or of our policies, or acting in an abusive way towards our employees or users;
- (…)"

Although cyber-harassment is not named as such, it does fall within the behaviour mentioned above.

5 Internet, Deep Web and the Dark Web

When talking about the cyber-problems that can happen in cyber-space, often it is mentioned that they occur in the Deep Web or the Dark Web without differentiating between the two. The problem with talking about this term, specifically **Deep Web,** is that it is taken as a given that even knows what it is, but it creates a lot of confusion and is often confused with the term **Dark Web**.

The **Deep Web** is the name given to the group of internet pages that do not appear on traditional search engines like **Google** or **Bing**. Pages that can only be accessed if you know their web address or URL and that normally deal with illegal and controversial topics such as contraband, the cyber-trafficking of people and terrorism and it is because of this that they do not appear on search engines.

It is called "deep" because that is exactly what happens on those pages. They are on the internet, just like every other web page, but not everyone can access them, they are not on a visible layer and they do not reach 90% of cyber-users.

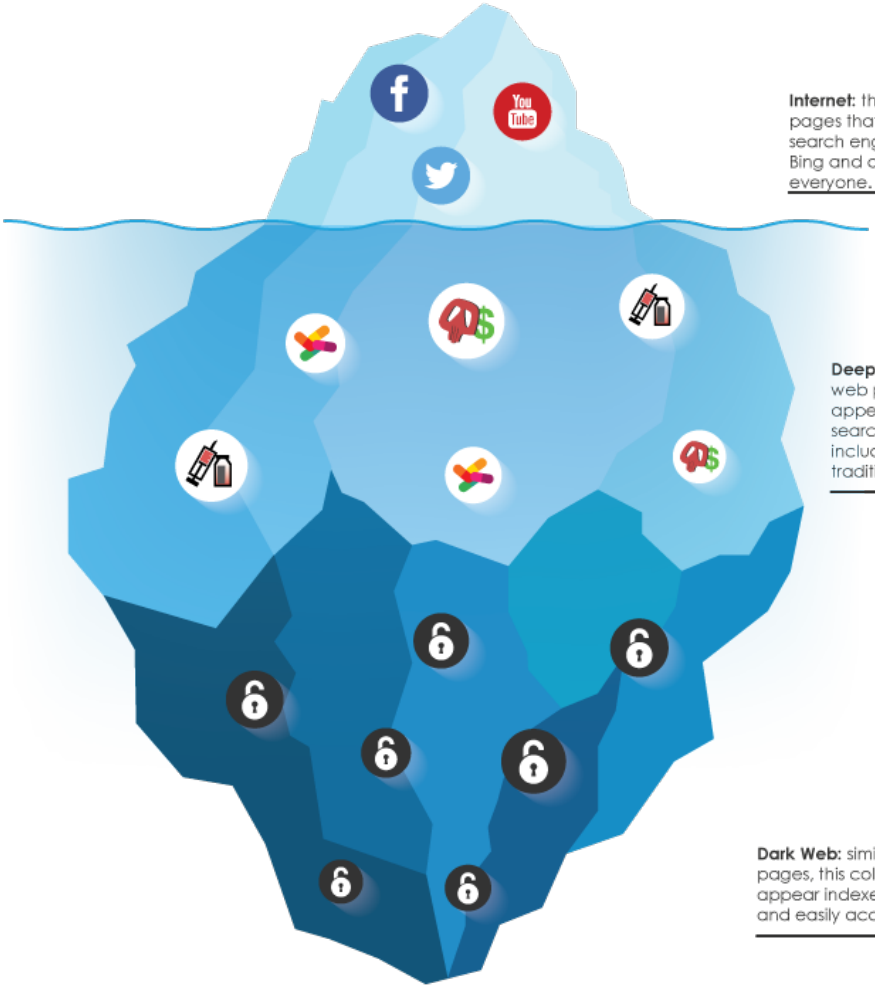
On the other hand, Dark Web (also called Dark Net) is also the name given to a group of web pages, but this time they are restricted and can only be accessed with authorisation and via certain contacts or systems (proxy systems, VPNs or authentication). Illegal and controversial topics are also found on these types of pages.

And so we are faced with the fact that under what it is usually known as the **Internet**, which for this case can be described as the group of web pages which may be accessed freely and are indexed by search engines, there are other layers of information consisting on other web pages that are hidden from the vast majority of cyber-users.

Why do they not appear on the "surface"? And why are they not visible to everybody? One reason is the people responsible for them do not want them to be visible as they deal with the buying and selling or drugs, substances, weapons etc. that may attract the attention of the authorities. On the other hand, precisely because of the content of these pages, the search engines do not want to make them visible.

When asked the question of if the average user risks accidentally accessing a Deep Web page (being as though by definition you cannot enter a Deep Web page even by mistake) and alerting the authorities, it is important to emphasise that **it is very complicated, nearly impossible even, to accidentally go onto one of those pages, therefore with normal internet usage there is no risk of entering one of them.**

Using **Google**, **Bing** or **Yahoo** to search on the internet, as well as common sense; and bearing in mind the precautions that we have already dealt with, we can use the internet without any problems regarding those types of pages.



Internet: the collection of web pages that appear on regular search engines such as Google and Bing and are accessible to everyone.

Deep Web: the collection of web pages that does not appear indexed in traditional search engines, they tend to include conflictive or traditionally illegal topics.

Dark Web: similar to the Deep Web pages, this collection of pages does not appear indexed, but they are not freely and easily accessible either.

6 Key antisocial behaviour on the internet II

6.1 Human Trafficking

Human trafficking, also known as the trading of human beings or people trafficking is currently one of the crimes which have experienced the greatest growth. With the appearance of the internet, their networks have been able to expand to every corner of the planet, to the point of becoming a global problem.

6.1.1.1 Scenario

The definition for people trafficking in the **physical world** was given in the **Convention against Transnational Organised Crime**, promoted by the United Nations in 2000 in Palermo, Italy:

"Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs."

Meaning that people trafficking is using deceit or violence, together with the transportation of people from one place to another to then later exploit them.

It is important to distinguish this from the trafficking of migrants, as this consists of somebody illegally entering a foreign State to obtain a material or financial benefit. These two issues are different concepts. With the trafficking of migrants, the victims voluntarily consent, without ending in exploitation and there is always an element of transnationality.

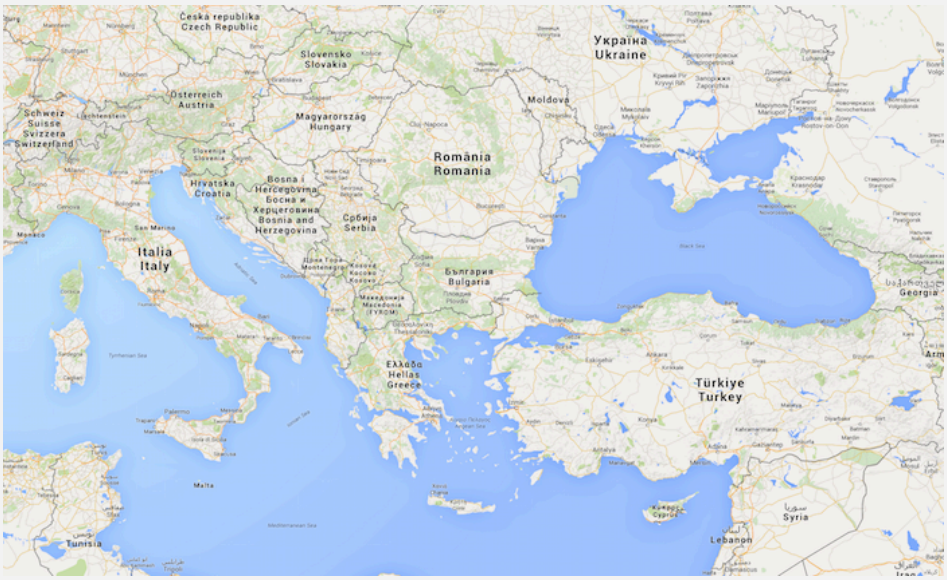
On the internet this is different as physical transport does not exist. However, the web can be used to **contact** and **capture** people in a way which makes them accessible in the physical world for the crime to eventually be committed. The internet is used to contact possible victims, and once this access is achieved, the transportation and subsequent exploitation, whichever form this may take, happens in the physical world.

The web can be referred to as one of the means by which trafficking begins: the crime is prepared and the victim is selected.

Following the lines marked out by the United Nations, the **Cyber-trafficking of people** could be defined as the activities of attracting and misleading of the victims, by means of threats, coercions, fraud, deceit, abuse of power and of a vulnerable situation or by means of the concession of receiving of payment or profits to obtain the consent of a person that has authority over another, with the aim of later moving, transporting and/or housing these people to then exploit them in the widest sense of the word.

As it currently stands, human trafficking moves in figures that are close to 30,000 million dollars. It is difficult to quantify these dimensions on a global scale, but it is believed that annually some 800,000 people[1] are the subject of trafficking over international borders, at the same time many other are exploited within the borders of their own countries. As the internet infiltrates more societies and corners of the globe, these figures grow each year.

DAILY NEWS 31/08/2015



The conflicts in Syria, ongoing since 2011, between the government and the rebels led to a constant surge of refugees in Europe in the months of June, July and August 2015. These refugees are trying to reach the borders of countries which are nearest to the war-zone, in the search of protection and asylum.

Specifically, thousands of people have tried to get to Turkey, Italy, Greece, Serbia, Germany and Hungary more than to other countries. This has ignited numerous collisions between the Governments of those countries, the authorities that are overstretched due to the arrival of so many people and the civilians that are trying to flee the war. Because of this, ever since Europe saw the massive arrival of individuals, the rate of human trafficking has noticeably increased.

The mafias dedicated to human trafficking and exploitation are making the most of the desperate situation that thousands of people are in. They do not let the refugees cross the borders, forcing them to pay for their transportation, or in other cases they promise them that they will transport them from one country to another but they end up being the subjects of human trafficking in distinct places to those agreed.

Together with the traditional methods for attracting victims, with the boom of social media and the internet, in the majority of cases these actions are carried out through the cyber-recruitment for the illegal trafficking of people; a cyber-conduct which takes centre-stage in current policies.

European authorities try to stop these criminals that make use of these networks to access refugees, promising them an escape route from the country, achieving a slow but sure advance against the traffickers. In Germany 1,785 traffickers were arrested in 2015 and the traffickers are being encircled more and more each day. However, at the moment nothing is being done in cyber-space to achieve the desired results to stop the recruitment of refugees.

[1] Source, International Organization for Migration

6.1.1.2 Analysis

In a territorial sense, the majority of States regulate this conduct in line with the foundations marked out by the Convention against Transnational Organised Crime and the protocol which was then signed to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children.

The States not only class trafficking as a crime, but they promote the protection of privacy and identity of the victims, the adoption of appropriate measures which allows them to stay on their territory and the establishment of mechanisms for the prevention and exchange of inter-party information.

And so, two types of legislation have been gathered in this sense, on the one hand the creation of Ad-Hoc Laws for sanctioning this behaviour, or the creation of special articles or sections within the already existing general Criminal Codes.

For example, in the State of **Texas, USA** there is a very similar definition in the Criminal Code to that of the Convention, and it is classed as a serious second degree crime with a maximum prison sentence of 20 years and a minimum of 2 years, as well as the imposing of a maximum fine of 10,000 dollars, according to sections 20.A and 12.33 of their Criminal Code.

But, for example, also **Spain**, lacks a law which facilitates the fight against and prosecution of this phenomenon. However, in this case the Framework Protocol for the Protection of Victims of People Trafficking (28 October 2011) has been signed and the treatment of which is extensively found in detail in the Criminal Code.

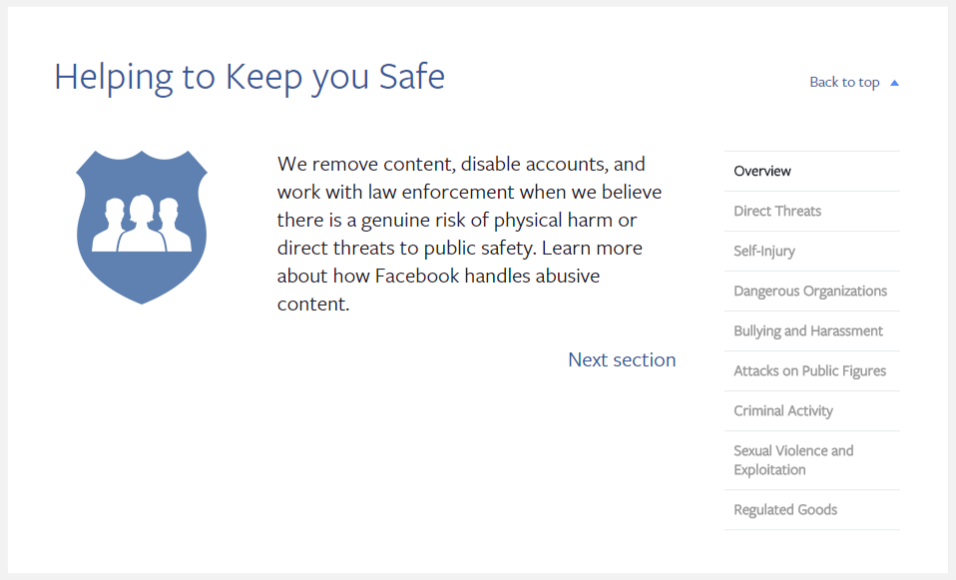
We can find many examples of ad-hoc laws in Latin American countries, such as Chile, Mexico and Argentina for example.

Lastly, for this analysis it is very important to mention the two international organizations in charge both of the surveillance and control of the application of these rules in the different States, as well as ensuring progression in the fight against people trafficking: The United Nations Office against Drugs and Crime, and the International Organization for Migration (IOM).

If we take the field of the **internet**, given that the cyber-trafficking of people can be carried out through the contact with and access to other people and through other behaviour such as deceit, abuse or blackmail, the way of regulating this conduct is via the demonstration in one of those.

In this regard, on **Facebook** for example, the treatment of a criminal activity by the users is carried out by means of the Terms and Conditions and the Community Regulations, but effectively people trafficking is not specifically mentioned. These terms prohibit:

- Intimidating, disturbing or harassing other users.
- Using the service for illegal, deceitful, malicious or discriminatory acts.
- Publishing content or carrying out any action on Facebook which infringes or violates the rights of third parties or that violates the law in any way.



Example of how Facebook prohibits criminal activities. Source: https://www.facebook.com/communitystandards

People trafficking on the internet falls into these prohibited actions, therefore it is a behaviour that is implicitly prohibited and perpetrators can be prosecuted in the same way as for the actions that the platform prohibits.

Another example could be that of **Line,** which, in its Terms, prohibits:

- Any activity which violates the laws, regulations, government requests or legal systems.
- Any activity that promotes illegal activities or disturbs public order, or that is considered as abusive, damaging or inappropriate.
- Announcing, transmitting or requesting any kind of information, message or content that is illegal, harassing, bothersome, threatening, abusive, discriminatory or in any way objectionable or offensive.
- Using the service for sexual means or for obscene acts, using the service to meet other users in order to have sexual relations and the harassing or slandering of other users; as is using the Service for other means other than the Service's true intention.

The rest of the organisations follow a similar system to the one above. **Linkedin** and **Whatsapp** prohibit threats, extortion and deceit, and what is true is that little by little this behaviour is starting to be distinguished from that which makes it up. It is likely that in the future specific procedures will exist to warn about it and prohibit it from being carried out on the internet.

6.1.1.3 Proposed solutions

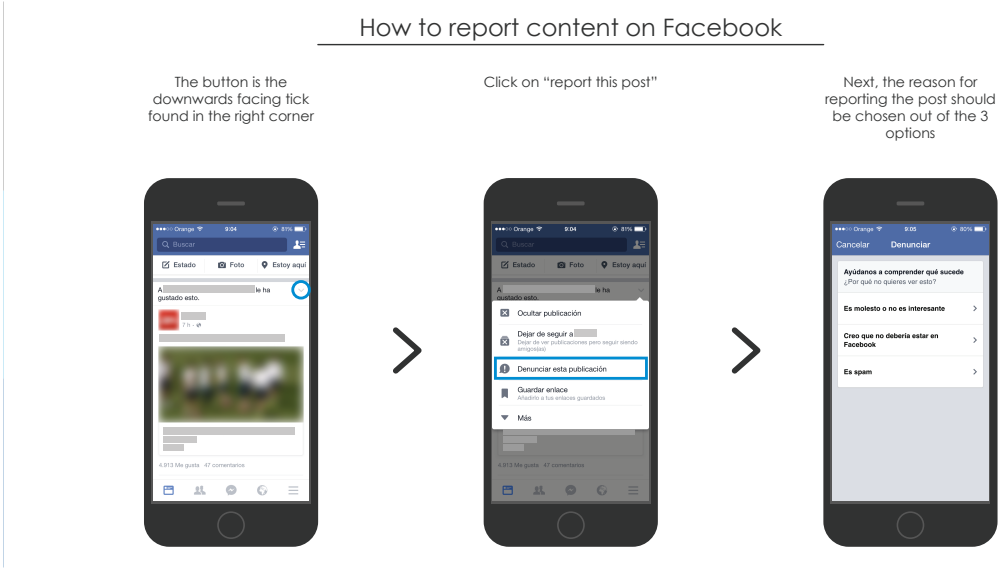
The proposed solution to deal with the problem of human trafficking is principally the support of a group action on behalf of those States that are directly involved with the migratory problems that are currently taking place.

An initiative which would jointly, and with the consensus of all its participants, approve the creation of supranational regulations to fight this issue would be the most appropriate path to take to solve it.

Of course, this is providing that the initiative had the aim both of enforcing prison sentences on those people and organisations that carry out human trafficking, and also the enforcing of cyber-sentences, banning internet use (cyber-prison) based on specific locations. For example, at interstate borders, where the majority of recruitment takes place for people who are later victims of human trafficking.

From the point of view of the cyber-organisations and the individuals, the main way of combating people trafficking is by teaching about the ways in which it happens, especially to the most vulnerable people (minors). It is very important to know that there are trafficking networks and a modus operandi when it comes to recruiting and selecting victims.

This means that people should be trained about how to correctly react when faced with situations that may amount to this type of crime, both in terms of how to deal directly with the possible perpetrator and how to report it to the cyber-organisations and authorities.



6.2 Drug and Medicine Trafficking

Drug trafficking has become one of the biggest focuses of criminality. It is currently estimated that it has been confirmed as an antisocial, prosecutable behaviour which moves thousands of millions of euros each year and has as big a presence in the physical world as it does in the cyber-world.
The trafficking of medicine is, together with drug trafficking is one of the most spread out conducts in the realm of trafficking products or substances both in the physical world or via the web.

6.2.1.1 Scenario

In the physical world, the illegal trafficking or drugs involves the illegal trading of and related activities regarding substances which are banned by law, this can be both within the borders of a State, or outside them. This is also known as **drug smuggling** or **drug dealing**.

The group of activities that define this activity are:

- The cultivation, manufacturing and elaboration.
- The importing and exporting.
- The distribution and trafficking.
- The sale or delivery.
- The promotion, encouraging and facilitating.

The **trafficking of medicines** consists of the illegal trading of products and substances that are classed as medicines or drugs, both within the borders of a State, or outside them.

This includes all those drugs which require a medical prescription or authorisation to obtain them, as well as those that can be gotten without any paperwork or requests.

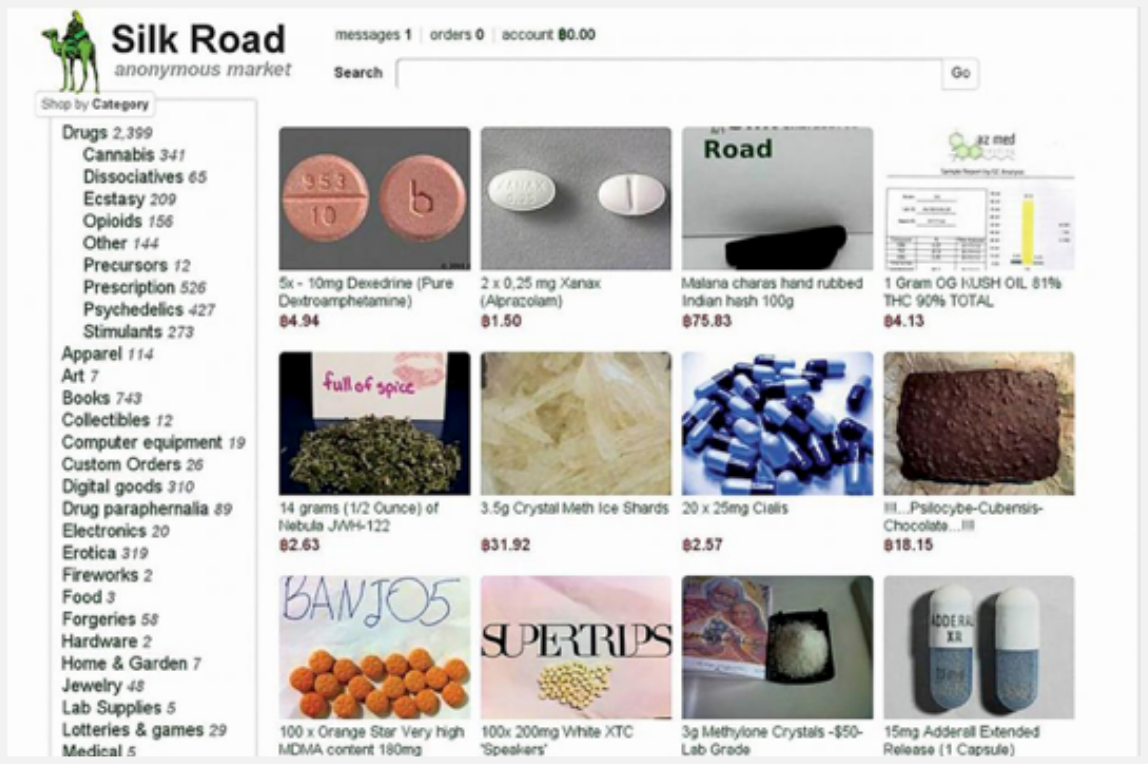
It is differs from trafficking of illegal drugs in the type of substance that is being trafficked. Whilst medicines are approved, tested and controlled substances, illegal drugs as substances that lack this approval, testing and control.

It is also possible that the trafficking of medicines included the distribution of adulterated drugs which have lost their properties and effects with health benefits, for example vitamins, medication for sexual dysfunction (Viagra) or antibiotics.

On the internet, this behaviour occurs through the distribution and sale of already manufactured substances and those being made available to buyers via trading websites available online.

The web is like a shop window for drug trafficking businesses and it is a meeting point between them and the buyers. In the cyber-world the substances that arrive are already made and ready for the transactions and direct consumption. Furthermore, cyber-traffic has become one of the most important activities in the "Deep web", meaning the part of the internet is not found via search engines.

Just like shops that legally sell other products in the physical world, true giants of illegal trading can be found in the Deep web, trading substances such as "*Silk Road*", and moving millions of euros each year thanks to the transactions that are carried out over the web:



Silk Road, the most well-known online market for the trading of drugs and medications.
Source: http://www.wired.co.uk/news/archive/2013-11/07/silk-road-2

Among those activities, the following can be highlighted:

- The distribution and trafficking through forums and websites.
- The selling or delivery via online transactions.
- The promotion, encouraging and facilitating.

This trafficking of substances includes a typology and a variety of substances that are trafficked without limits, just with a subtle difference:

When referring to drug trafficking, this in reality includes a multitude of different substances, such as narcotics, substances that come from plants such as cannabis, mushrooms or cocaine, methamphetamine, steroids, crack, poppers etc. All substances that are prohibited or controlled by the authorities in each State.

Whilst on the other hand the trafficking of medicines includes:

- The trafficking of all types of medication through prohibited channels (fraudulent websites, websites with aims other than trading, etc.)
- The trafficking of false, prohibited or out-of-date medication through any kind of channel (both legal and illegal) in a scenario very similar to that of cyber-piracy.

To get an idea about the magnitude of the problem according to the World Drug Report by the UNODC (United Nations Office against Drugs and Crime[2]) together

[2] World Drug Report 2014. UNODC

with the WHO (World Health Organisation), it is estimated that the current number of people that consume some kind of illegal drugs is between 8.9 million and 22.4 million, with a higher rate of incidence in the East and South of Europe.

In terms of medicines, according to data from the World Health Organisation (WHO), 1 in every 4 medicines is false, and this percentage is higher in developing countries, with figures reaching almost 90%.

Finally it is worth stressing the figure of the key agent and protagonist at an international level regarding the trafficking of drugs and medicines, the UNODC (the United Nations Office against Drugs and Crime), whose role is crucial when combating these activities.

6.2.1.2 Analysis

The regulations of both conducts has different treatments both in the real world and cyber-world, meaning both within the different territorial regulations and with organisations' cyber-rules.

In terms of territorial regulations, of all the States that were analysed, all of them punish trafficking of legal and illegal with fines and prison sentences depending on the seriousness of the circumstances. The majority of States have special laws within their Criminal Codes that address this behaviour.

In **Spain,** for example, the Criminal Code punishes the actions of promoting, encouraging and facilitating the consumption of illegal toxic or narcotic drugs or psychotropic substances with prison sentences of 3 to 6 years.

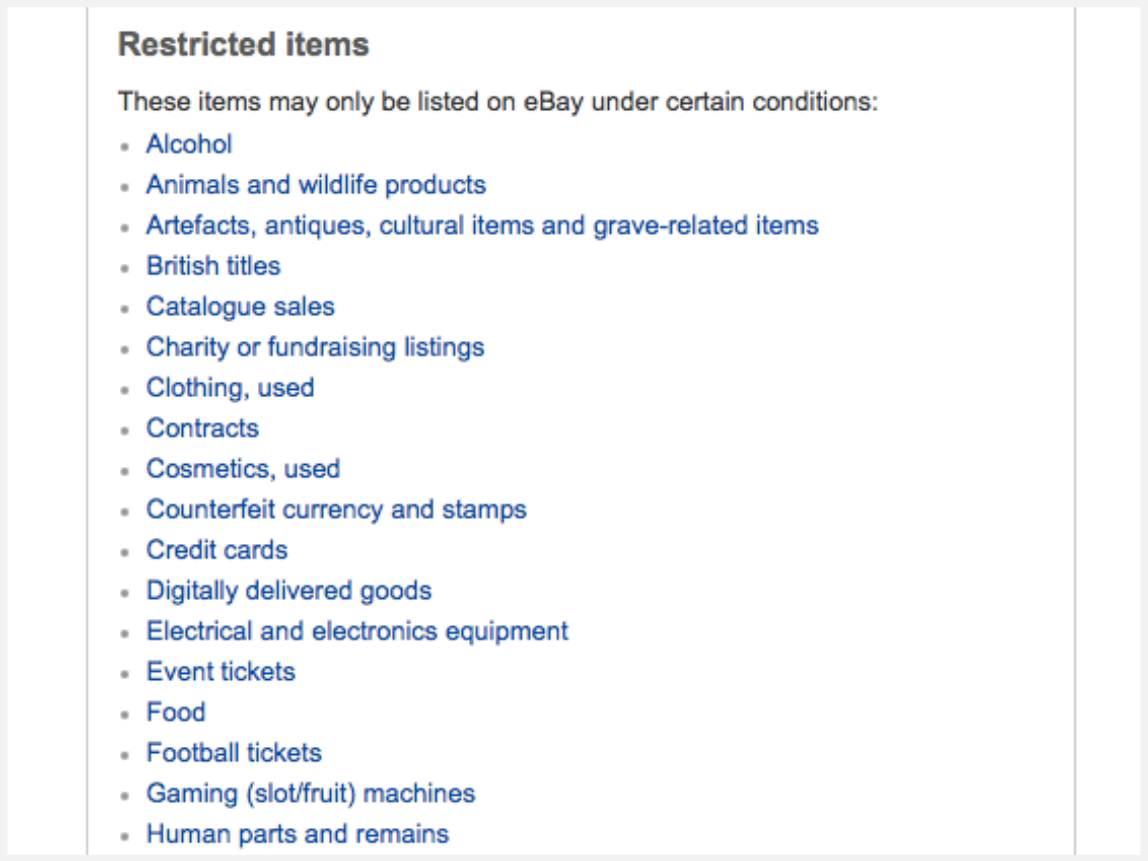
In **Mexico**, the Criminal Code also establishes in section 194 that the actions of transport or trafficking, trading, supplying, prescribing or introducing or removing from the country this type of substance are punished with prison sentences of 10 to 25 years, or 4 to 7 years if they are not considered to be destined to carry out one of the behaviours mentioned in section 194.

And, as another example, in the State of **California** in the **USA,** sections 11350 and 11377 of the Health and Safety Code establish that the mere possession of a narcotic or illegal substance is a serious crime and, unless there is a written medical prescription, it is punishable with up to 3 years in state prison. In the case of trafficking and promoting, according to sections 11352 and 11378 of the Health and Safety Code, this is punishable with up to 5 years in state prison.

In terms of the legal system in **Cyber-world**, the activity of the cyber-trafficking of medicines mainly takes place on the "Deep web", as does the cyber-trafficking or drugs, however it also takes place to a lesser extent on online trading websites, and thus the positions of the key organisations of the exchange of goods must be taken as a reference. It is those organisations that provide users with the mechanism, the shop window and the ease when it comes to trafficking drugs and substances online.

In this regard, entities such as Amazon, Ebay and Milanuncios play a crucial role in the control, prohibition and prevention of this behaviour.

Given this importance, they dedicate an extensive part of the organisation of their websites to regulating and prohibiting this behaviour. For example, **Ebay** prohibits everything from the most common and well known substances such as cocaine, marijuana, hallucinogenic mushrooms or narcotics to those elements that can be used for the commission of crimes that drug trafficking involves or leads to. As such, the trading of pipes for smoking is not allowed, regardless of the type and class, neither are (apart for the odd exception) papers used for smoking, syringes or needles, for example.



Restricted items

These items may only be listed on eBay under certain conditions:

- Alcohol
- Animals and wildlife products
- Artefacts, antiques, cultural items and grave-related items
- British titles
- Catalogue sales
- Charity or fundraising listings
- Clothing, used
- Contracts
- Cosmetics, used
- Counterfeit currency and stamps
- Credit cards
- Digitally delivered goods
- Electrical and electronics equipment
- Event tickets
- Food
- Football tickets
- Gaming (slot/fruit) machines
- Human parts and remains

Some of the items that are restricted on Ebay.
Source: http://pages.ebay.co.uk/help/policies/items-ov.html

Similarly, **Milanuncios** does not allow content to be available that is formed of narcotics, drugs, hallucinogenics or any other substance that is not permitted by the law in force. In addition, it also prohibits utensils that are used to produce, consume or promote consumption, distribution and production of these substances, and it prohibits actions which directly promote drug consumption.

Another example is that of **Aliexpress** whose contents policy establishes in the Terms and Conditions that the following products, among others, cannot be published:

- Adverts for prescribed medications, narcotics, steroids, drugs, medical products and moreover, adverts that offer medical or health care services, including services for medical treatment, rehabilitations, vaccinations, health checks, psychological or dietary advice, plastic surgery and massages etc.

The conduct of medicine and drug trafficking over the internet is clearly banned, with all of the possible options being grouped together in one clause.

6.2.1.3 Proposed solutions

The path to eradicating the drug and medicine trafficking online have been mainly focused on analysing the deep internet or "Deep web" that cyber-criminals use so as to not be found and that is also useful for consumers to be able to acquire these substances over the internet.

The police and security forces in each State, along with the organisations, should create a research and monitoring body of the Deep Web, and of the cyber-markets for the trafficking of drugs on the rest of the internet, in such a way that the merchandise in the physical world could be traced, as well as the traffickers.

In an incognito way, or by using an agent disguised as a buyer as a bait, the objective is to make contact with the networks of cyber-trafficking of drugs and to be able to physically act against them, as the operability on the Deep Web of this type of networks is difficult to attack from the network itself.

In terms of the companies that own the medication, those known as pharmaceuticals, it is required that they carry out virtual services or cyber-surveillance to monitor and detect the uncontrolled selling of their products.

This is because those that go under the radar of the controls in distribution that happen in different territories, once they get to the minority distributor, or even by an internal route, the it is permitted to commercialise these products that have not undergone the control in the production chain.

DAILY NEWS 06/08/2015

Systems for the trading of medications over the internet are now available all over Europe and Spain. These will allow buyers to check that they acquire their medicines in a legally authorised pharmacy and that medications sold are of the guaranteed quality, security and efficiency necessary.
The system is based on the each pharmacy or establishment having official authorisation from the State in such a way so that they can sell certain medications (only those that do not require a prescription) over the internet, and the inclusion on this trading web page of the official logotype, through which it can be verified that the purchase is carried out with guarantees. This logotype will be interactive and will allow users to access the list of establishments in each territory that can sell the goods.

Additionally, the Spanish Agency of Medications and Healthcare Products (AEMPS) has opened the DISTAFARMA portal: www.distafarma.aemps.es where:

- The establishments can manage their requests to obtain the certificate
- Users can consult the authorised establishments in terms of Provinces and Autonomous Communities
- Users can consult the frequently asked questions.

This system is a powerful and solid element against the illegal cyber-trafficking of goods which uses the lack of control of the organisations that work over the internet and the lack of authorisations as their key point of strength. This will permit institutions to control part of the trafficking of drugs that happens online and it will eliminate part of the illegal transactions that occur on the web.

6.3 Cyber-Laundering of Money

In reference to the crimes and incidents regarding, assets, goods and money, money laundering is one of the most well spread conducts within the criminal world, and its existence causes severe consequences to the economies that suffer from it.

Throughout 2014 and 2015 in Spain a scandal was uncovered in the banking entities Banca Privada de Andorra (BPA) and its affiliate Banco Madrid, for their supposed collaboration with the money laundering of an organised crime. This forced the Andorran and Spanish authorities to impose temporary financial limits on the group after the loss of savings that the entity has suffering.

The discovery of these activities led the administrators to request that the entity went into administration and that their operations were suspended until the legal bodies had decided on the future of the bank, leaving their deposits, investment funds and SICAVs blocked, at present this issue has not been resolved.

Examples such as this can be seen on a daily basis in many other States in the world, as such this is not an isolated case of little importance.

6.3.1.1 Scenario

Money laundering refers to those operations that aim to transform goods, money or assets from an illegitimate or illegal source into lawful, transparent products. Another one of the objectives is that if this objective is not achieved, the goods at least appear to have those characteristics.

The most important element in money laundering consists in the working with funds, goods and assets which are the fruit of illegal or criminal activities, with knowledge of such. If talking about money which is legally registered or was not born out of activities such as terrorism of drug trafficking, it cannot be referred to as laundering.

These goods are often referred to as "black money" and they are those that the criminals aim to "clean" or "launder".

Despite the diverse methods, various phases or steps in a laundering operation can be identified, they include:

1. The carrying out of a criminal act and the obtaining of assets, goods or money.
2. The introduction of the product in the financial system.

3. The carrying out of operations to hide the source and to make it difficult to trace.
4. The final integration of the money in the banking system; the peak of appearing legal.

On the internet, cyber-laundering happens by means of offering victims and third party collaborators deceitful of fraudulent businesses, operations and offers so that they operate with different assets and the manage to introduce them into the financial system. The cyber-laundering happens both through the abuse towards victims and with the collaboration of third parties, and the role that the internet plays is the support and base for both types of activity.

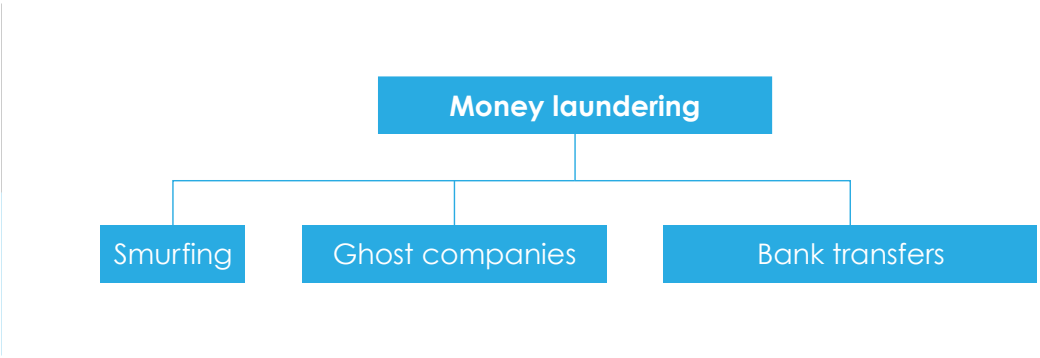
The cyber-laundering of money over the internet can be, in certain cases, carried out from the first moment that the criminal act takes places (through the robbery, fraud, scam for example) until this money is integrated in the financial system of the State where the events took place. In other situations, the internet is not used until a later moment in which certain actions or transactions have taken place, such is the case with the laundering of non-monetary goods. (For example, when trafficking with stolen products, first the robbery or theft is committed to then be able to trade these products, these days this mainly takes place online).

The most common forms of money laundering, both in the physical world and the cyber world are the following:

- **Smurfing:** Consists in dividing illegally sourced money into small amounts, in such a way that the transactions are more difficult to control, register or they simply do not appear suspicious.

- **Ghost/cover companies:** The creation or using of business organisations in a seemingly legal and normal way, but that actually are used to launder money that had been obtained illegally or fraudulently and that do not carry out any other activities.

- **Electronic or bank transfers:** Carrying out transfers on the internet to move money from one account to another, between countries so that the money is difficult to trace and its origins are hidden.



6.3.1.2 Analysis

For the territorial world, in the majority of cases laundering is addressed in special laws dedicated to these types of crimes, together with the financing of terrorism and other related crimes. As such, legal similarities can be found within different countries, for

example in **Argentina** there is Law Nº 25.246 on the concealment and laundering of criminally sourced assets, which modifies the Criminal Code; compared with the ensemble of laws that can be found in **Switzerland**, a State which has been traditionally linked to money laundering, with the Federal Law on the Fight against Money Laundering in the Financial Sector (Anti-Money Laundering Law, AMLA) and the provisions within the Criminal Code.

For the most part, the classification of these cases is based on the same prohibited conduct, this tends to be the transformation of money or goods which have arisen from a crime; hiding, altering or making the traces and evidence of such disappear, as well as the prohibitions of helping third parties to dodge the investigations of the relevant authorities or the covering-up or lack of reporting of being witness to an action of such.

The punishment of sentence is the differentiating element, as so, taking the examples shown above, we can find prison sentences of between 6 months to 3 years for these crimes in **Argentina**, whilst in **Switzerland** this is more harshly punished with sentences that range between 3 to 5 years (sections 260 and 305 of the Swiss Criminal Code).

Cyber-laundering moves so much each year that it is impossible to determine how much.
Source: depositphotos

In the cyber-world the fight against cyber-laundering has an advantage in that it is a limited occurrence to certain organisations due to the facts that transactions of assets and money are not easily carried out over their web pages.

And so, the focus of surveillance and control has to be limited to organisations that offer goods trading services, such as **Ebay** or **Mercadolibre,** professional contact and

employment portals such as **Linkedin**, and of course, financial organisations and entities or those with electronic money.

On **MercadoLibre** the publication of the following products and services is prohibited:

- Stolen products.
- Objects which are classified as historical heritage.
- Financial loans or credit.
- Legal tender, bank accounts and bank deposit services.
- Shares, bonds, titles or any other paper that is listed on the Stock Exchange.
- Credit and debit cards, whether valid or not, and the services to obtain such cards.
- Card payment terminals, readers and card code duplicators.
- Replica coins and notes of ones that are in circulation.

Example of MercadoLibre's Terms and Conditions.
Source: http://ayuda.mercadolibre.com.ar/ayuda/Articulos-prohibidos_s1028#1034

On **Linkedin**, transactions which are not what the platform is designed for are directly forbidden:

- Renting, leasing, doing business, selling, re-selling the access to services of any other related information or data.
- Selling, sponsoring or obtaining an economic benefit from the LinkedIn group of any other function of the Services without the permission of LinkedIn.
- Acting in an illegal, offensive, abusive, obscene or discriminatory way or any other condemnable way.
- Creating or operating a pyramid scheme, fraud or another similar practice.

To finish off this analysis, it is necessary to mention that, just like with regard to people trafficking, the Convention against Transnational Organised Crime, promoted by the United Nations in the year 2000 and which took place in Palermo, Italy, is relevant in this regard. As a result of these meetings, protocols were signed requiring the different signing countries to: establish different internal regimes to regulate and supervise the banks, financial institutions and bodies which are susceptible to be used for money laundering; to maintain transparency and information guarantees; and to adhere to international surveillance and cooperation.

6.3.1.3 Proposed solutions

In order to avoid the spreading of the cyber-laundering of money as a crime on the internet, as series of measures should be put in place that primarily aim to establish a **control over the activities and operations on the net**.

This role should be assigned, almost exclusively, to the banks and building societies, which should have the backing of the different State bodies and the Central Banks in the different States.

The work that they carry out should have the aim of promoting and performing:

- Surveillance and control of activities, as this has a role in guaranteeing the legality of every transaction made through their services. They should monitor and report and suspicious behaviour, and for that it would be particularly fitting to create inter-company surveillance and control committees in those companies and sectors that are susceptible to suffer from these issues.
- The creation of different bodies that are exclusively dedicated to controlling financial operations, such as the Financial information offices that can already be found in many States and are a good example of this type of organisation.
- The creation of cyber-offices for the surveillance and control of the different organisations that exclusively work over the internet.
- Likewise, they should be the principal actors in the framework of the creation of international agreements for the prosecution of this cyber-behaviour.

Example of the State body for the fight and prevention of Money Laundering.
Source: http://www.sepblac.es/espanol/home_esp.htm

6.4 Hacking

The term hacking is socially controversial. It could be designed as the group of techniques that are used to access a computer system (taking this in its widest sense), violating the originally established security measures.

The person that has a high amount of knowledge in computer security and is capable of carrying out the techniques outlined above is referred to as a hacker. Depending on their ethics, they can be classified as WhiteHats Hackers, who use their knowledge to improve security systems and correct vulnerabilities; or as BlackHats Hackers, who prove their knowledge by exposing deficiencies in external systems which imply a serious risk for cyber-organisations and internet users.

Although generally speaking when *hacking* is spoken about it tends to create the illusion of illegal access; it should not be ignored that actually *hacking* is nothing more than the series of techniques that are used to gain access to a computer system by violating its security measures, regardless of the aim of doing so.
Therefore this access does not, in the first instance, necessarily have to be classed as illicit or illegal, it could be that the introduction into the system forms part of a contractual

relationship whose aim is to test the robustness or check the weaknesses of the security measures of the ICT system of a company (as is the case with ICT security professionals or the ethical hacking techniques).

This is oldest cyber-behaviours as it came about almost at the same time as computer science due to the hacker's curiosity to known the workings of computer systems in depth.

6.4.1.1 Scenario

According to the Spanish national newspaper El País, "2015 may already be labelled the year of the *cyber-crime*". Furthermore, during the first quarter of 2015 both Kaspersky Lab and PandaLab – two of the laboratories that belong to successful antivirus software companies- emphasised that cyber-criminality was on the rise in an astonishing way.

It should be mentioned that as a result of the hacking techniques, other types of reprehensible behaviour have emerged, such as cracking, the use of malware of spyware, the access to content without consent, etc., which will be analysed in more detail later on.

Hacking is a behaviour which solely belongs in the cyber and internet worlds. It cannot exist in the physical world because of the electronic devices needed (computers, tablets, smart phones, wearables etc.) and the internet access that is required. However, that is not a reason for the regulations in the territories to not intervene.

Out of all of the behaviours in cyber-space, this is one which occurs the most. In fact, the term "hack" is now often seen in the media- as in the Ashley Madison case- with its main reason being that it was a pioneer for other similar cases.
Whatever the time or context, examples of news stories can be found which illustrate the above point: For example, in February 2015, the Chilean 24 hour news portal reported that, "Users of social media reported that during the night the Chilean Ministry of Defence website was attacked with messages that inferred to Islamic State and the current conflict in the Middle East." Furthermore, during the intervention messages could be seen such as "Saddam Hussein", "We are ISIS", "There is no other God than Allah"; and more recently, on 8 October 2015, the BBC Mundo portal led with the headline "the worrying vulnerability of nuclear power plants at risk of computer attacks", showing that these attacks are a reality that we live alongside.

6.4.1.2 Analysis

From a territorial point of view, due to the longevity that was mentioned in the introduction, there are already a lot of regulations which punishes this behaviour when carried out maliciously, such as for example when there was no consent for the infiltration in a computer system.

For example, in **Spain**, the Criminal Code penalises, in section 197 bis, anyone that by any means, or by violating the established security measures to stop this, accesses of facilitates another's access to a computer system. This is punished with a prison sentence of six months to two years. Likewise, the creation of programmes which facilitate or allow

for the illegal access of a computer system, or making this available to a third party is also punishable.

In the **United States,** and more specifically in the State of California, section 502 of their federal penal code prohibits the unauthorised access to computer systems, alluding to various special cases, and for each of them it states the corresponding fines and even prison sentences.

In terms of European legislation, the French legislation could be given as an example, specifically Law 88/19 of 5 January 1988 which verses on computer fraud and sanctions both the access to the computer system and the permanence on it; it also increases the punishment should there be any modification of or suppression to the information on the system, or if the system is altered at all.

South American legislations also consider this behaviour as a crime. For example, in **Peru** the Law 30.096 from 2013 punishes, with prison terms of between 1-4 years, anyone who, without authorisation or with sufficient authorisation, accesses a computer system which is protected with security measures that have been violated.

After an exhaustive analysis of the distinct territorial legislation, it can be deduced that the differences in terms of punishments come from the fact that certain legislations regulate the illegal access in an autonomous way, whilst others do so together other harmful conducts.

From the point of view of the cyber-world, hacking (understood in its harmful sense) tends to be banned, both in the general conditions and the terms of use that cyber-organisations make available to their users.

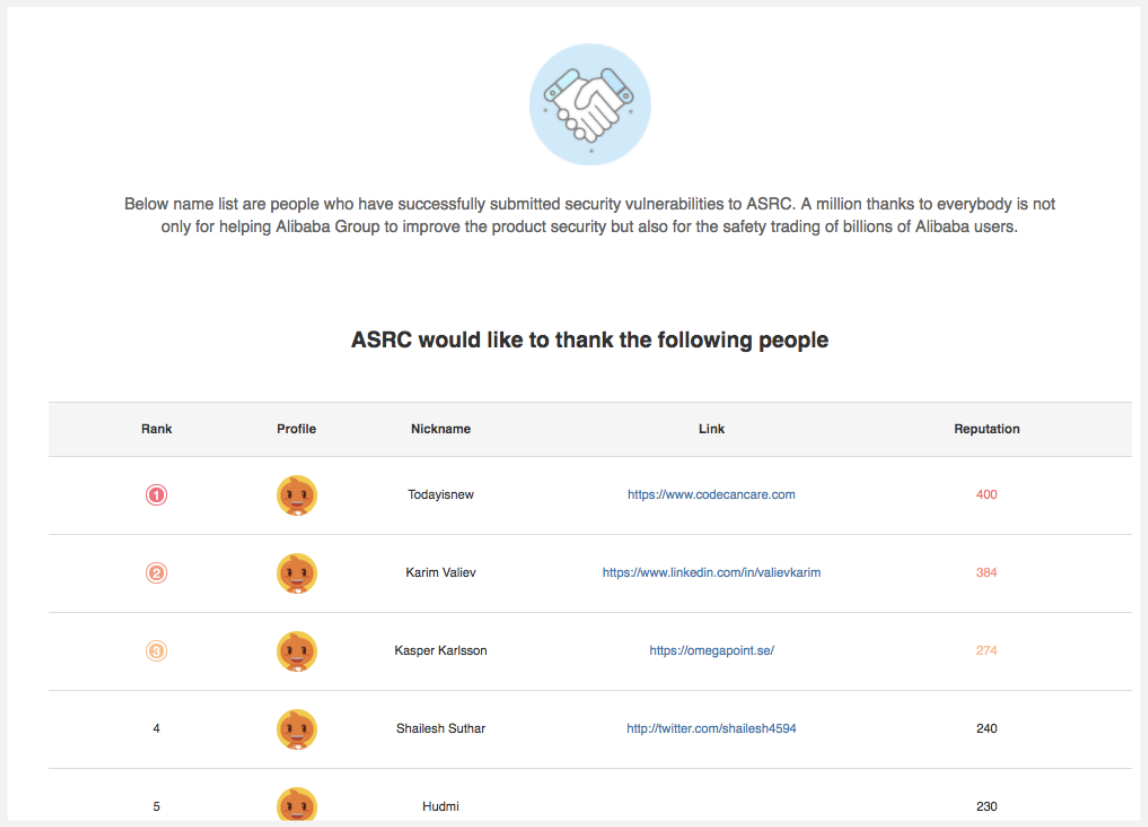
For example, the portal **Vibbo** (previously **Segundamano**) which is dedicated to the buying and selling of second hand goods, prohibits the commercialisation of devices of programmes that allow for what is written on the keyboard to be saved, such as: Keyloggers, keyghosts o keysharks; as well as password recovery services of the "hacking" of emails.

On the internet access portal **Terra**, it is highlighted that every user will avoid using the services for illicit or prohibited means or those that could damage, overload or impede the normal use of their computer equipment, documents, files and any kind of content that is stored on any one of the computers of Terra or another internet user.

Now, if the hacking is well intended, there are sites where they foresee the intrusion in their systems.

This happens on site such as **Linkedin and other platforms like Netflix,** where it is established that if a computer security professional wants to gain information about the weaknesses detected, they should know that there is a policy about responsible disclosure and as such the platform will not take measures against them for telling them about them.

In fact, one could even aspire to been on the honour's roll, like in the case of the Alibaba portal's Hall of Fame:



Below name list are people who have successfully submitted security vulnerabilities to ASRC. A million thanks to everybody is not only for helping Alibaba Group to improve the product security but also for the safety trading of billions of Alibaba users.

ASRC would like to thank the following people

Rank	Profile	Nickname	Link	Reputation
1		Todayisnew	https://www.codecancare.com	400
2		Karim Valiev	https://www.linkedin.com/in/valievkarim	384
3		Kasper Karlsson	https://omegapoint.se/	274
4		Shailesh Suthar	http://twitter.com/shailesh4594	240
5		Hudmi		230

The Alibaba Hall of Fame.
Source: https://security.alibaba.com/en/fame.htm

6.5 Cracking

The term "crack" in this case refers to the breaking of a system's security measures, and the aim the perpetrator has of doing this is to gain a benefit or simply to cause harm.

Cracking has a shared methodology with hacking as it also consists of the violation of established security measures. However, the intention and goal of the perpetrator of cracking is different, and in this case it is qualified as illegitimate, illicit and illegal. For this reason, and because the consequences change, and individual study of this is required.

6.5.1.1 Scenario

Cracking is an antisocial cyber-behaviour that involves accessing a system without the authorisation to do so, the consequences of such are the causing of damage or alterations to said system. This term is also used when talking about the violation of copyright protection measures of a computer system by means of reversed engineering techniques.

It is common for cracking techniques to come alongside other antisocial and criminal behaviour.

The damage that is linked to these types of cyber-attacks can be important: from the deactivation of certain systems or the entirety of a telecommunication network, to data robbing, information manipulation or the infection of other computers.

6.5.1.2 Analysis

From the perspective of the physical word regulations, the territorial legislations tend to sanction the cyber-behaviour of cracking as a crime, just as was analysed previously with regard to hacking.

Prison sentences are usually enforced, and fines can be imposed on top of them. However, however it is not common for cracking to be specifically mentioned, rather it tends to be penalised on a par with what is foreseen with the violation of a computer system's security measures, or it is dealt with together with another series of cyber-behaviours that can amount to diverse levels of seriousness; from there, the charges change according to the provisions within each legislation.

For example, in **Spain** the Criminal Code states in section 270.5 that anyone who deletes or modifies the technological measures for the protection of content will be prosecuted. The aim of this measure is to protect those that hold the intellectual rights to something from the so called "*crackers*", meaning those that violate the established anti-copyright measures of an specific software.

In the State of Connecticut, in the **United States**, the federal criminal code sets out a sub-section within sections 53a-251- which are exclusively dedicated to crimes committed via a computer, known as "computer crimes". Amongst other, the following are considered as crimes: accessing, without authorisation, of a computer system; intervening, without authorisation, in the computer services and; the malicious use of information contained with the computer system.

Chile, in Law no. 19.223 sanctions anyone who intercepts, interferes or accesses a computer system providing that coincides with intent of taking over, using or unduly finding out information that is contained in the system. Minor prison sentences will be imposed.

From a **cyber-space** perspective, the problem with cracking and the subsequent interest in its regulations is seen to a higher extent in those cyber-organisations that have a software or product available that protects against the cyber-criminal's intents at breaking it or passing through it.

For example, **Microsoft's** generic contract expressly prohibits the use of reverse engineering techniques, the decompiling and the disassembling of software. Likewise, in the framework of their contract it states that, in terms of the software and services, the user cannot have any contact with the technical protection measures that said software or services contain, or publish or copy the software.

Similarly, on the online games platform Pokestars.com, or on *economy sharing* and also on Blablacar.com, their terms of use prohibit the decompiling or resorting to reverse

engineering of the software. Something similar happens with Playstation which does not allow decompiling, reverse engineering or source code manipulation techniques. Furthermore, **Youtube** prohibits the evading, deactivating or manipulating in any way (or trying to do so) the security functions of their services or other functions that impede or restrict its usage, or the copying or content, or the application of usage limitations on the services or content that are offered via the services.

Looking at it like this, practically all of the cyber-organisations consider measures to alleviate these types of antisocial conducts, giving the users the possibility of reporting such actions in order to act against them as soon as possible.

6.6 Malware

Malware is the most frequent way of illegally entering an external computer system. Its variations of computer viruses and worms form part of the ecosystem against which internet users have to face each day.

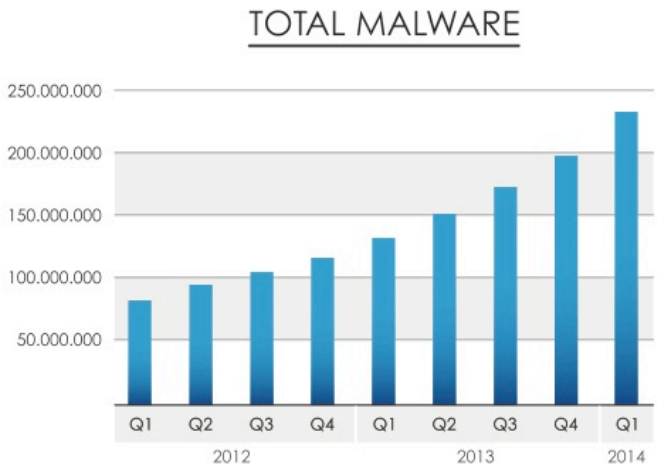
6.6.1.1 Scenario

Malware, is an abbreviation of "Malicious software", and it is the word used to describe all the programmes or malicious codes designed to be introduced, without the owners consent, into computer systems, causing harm, malfunctions and the stealing of information.

It includes a whole host of different subtypes, such as viruses and Trojans which have their individual peculiarities, action methods, configurations and effects, but the generic name for them all is malware.

The cyber-behaviour consists of trying to use a computer programme (malware) to use the system of a third party without their knowledge and with the aim of causing them direct or indirect harm, or benefiting oneself; therefore, it is a behaviour that exclusively belongs in the cyber-world. Just like with cracking, the use of malware tends to be a step to committing other cyber-crimes.

It is not just committed on computers, but it can also be designed to work on tablets, smart phones, storage devices, data centres, etc.



[3]

The most well-known varieties of malware are:

- **Viruses:** Malware designed to alter the normal functional of a computer without its owners knowledge. How it works is simple: it gets introduced in other systems through infected programmes, and it tries to inject its code in other executable programmes from the computer, the aim of this is to stay in the computer system for as long as possible. In order for it to infect other systems, the infected file has to be ran on an external system.

- **Internet worms:** A worm is a type of malware that, unlike viruses, does not need to alter the files of programmes to replicate, but it can make duplicates of itself. Worms almost always cause problems on the web as they are programmed to spread out, whilst viruses just infect or corrupt the files of the device that has been attacked.

- **Trojans:** This is a type of malicious programme that seems legitimate and inoffensive, but once used it allows the attacker to have remote access to the infected device and as such, all of the information that is contained within it.

- **Keyloggers:** a malware whose aim is to register and send to the attacker all of the information that is typed on the computer. Although they do not harm anything themselves, they put the privacy of the user at risk and they can collect sensitive information about the user such as bank accounts and passwords etc.

- **Botnets:** a malicious software that converts the device or computer into a bot or "robot" that then undertakes automatic tasks on the internet without the owner's knowledge. When there is a wide network of "robot" or "zombie" devices, this is referred to as a botnet. These networks tend to be used by cyber-criminals to send spam, spread viruses, attack devices and servers etc.

[3] Source: macafee report 2014: http://www.mcafee.com/mx/resources/reports/rp-quarterly-threat-q1-2014.pdf

- **Spyware:** A programme which is installed on a device without the consent or authorisation of the owner with the aim of gathering information to then send it to the attacker.

- **Adware:** The prefix "ad" in "adware" refers to the word "advertisement". Therefore, it is a malware that makes reference to programmes that intrusively and unexpectedly display publicity, usually by means of pop-up windows.

- **Ransomware:** This is closely related to cyber-extortion, they are programmes that encrypt files that are important to the user, making them inaccessible. The user is then extorted to receive the password to be able to recover their files. An example of this is CryptoLocker.

However, malware tends to combine diverse variants from those that have just been mentioned.

DAILY NEWS 06/05/2015

This is the case of Rombertik; a virus that starting causing havoc in May 2015 as it was made up of various specialised mediums, such as Computerhoy.com
(Look for a similar image with rights. We do not have the rights for this one)
It dangerous and unusual characteristic lies in the fact that, if it is detected by an anti-virus software on the PC, it is capable of completely deleting the hard drive.
Rombertik is transmitted via #spam and #phising and it fundamentally affects Windows systems. Once the spyware is installed on the computer, it stores all types texts that are written in the browser's windows. This allows it to gather the user's personal details, amongst other things.
But without a doubt, what is most characteristic of Rombertik is its ability to periodically check if it is being analysed or audited by an anti-virus. With just the slightest hint of this, it will try to overwrite the Master Boot Record (that is the first sector of the hard drive that seeks the previous computer to load an operative system), in such a way that if it does not have access to it, it will act as a ransomware, kidnapping and encrypting the files that we have on the computer.

6.6.1.2 Analysis

In terms of the analysis of the territorial regulations regarding malware, currently two different situations can be found. One is of those countries whose regulatory body has specific laws of computer-related crimes and one is of those countries in which the Criminal Code only includes those prohibited conducts.

An example of a country with specific laws is the **United States**. In more than 20 States, including New York, California and Nevada, there is legislation that aims at directly prosecuting spyware. Moreover, in the majority of the States, cyber-crimes are regulated

in a section within their criminal legislation, and malware is mentioned within their definitions:

> "**Computer contaminant**" means any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.
>
> They include, without limitation, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.4

In **Spain**, the Criminal Code states in sections 264 et seq. sentences to imprisonment anyone who produces, acquires, imports of facilitates it to others a computer programme which has the aim of deleting, damaging, deteriorating or altering computer data, programmes or electronic documents.

In **China,** section 286 of the Criminal Law of 1997 considers it be a criminal activity to create and deliberately spread a virus or other programmes that sabotage the normal workings of a computer system, this can be penalised by up to 5 years imprisonment should the consequences be serious.

In the **Dominican Republic,** law number 53-07 about high-technology crimes, states in section 8 that it is punishable to produce, use and distribute, amongst others, computer programmes, devices or material that has the sole use or fundamental use of being used as a tool to commit high-technology crimes and offences. These are punishable with prison sentences of 1 to 3 years and fines between 20 and 100 times the minimum wage.

In terms of the regulations in cyber-space, in every cyber-organisation it is easy to find the anticipation of prohibited behaviour regarding the use of malware to damage computer systems, whether the organisations' or the users'.

For example, **Blogspot** establishes in its General Usage Conditions the general rule that each user will undertake to use the services and contents of the portal in line with what is acceptable in terms of the law, morals and public order. It expressly establishes a list which entails a prevention against malware due to the fact that the user undertakes to:

- Not introduce or spread on the network data programmes, viruses and harmful software that is susceptible to cause harm in the computer systems of the access provider, their providers or third party users of the internet network.

Another example can be found in **Netflix's** Terms and Conditions of Use which specifies that it is not permitted to introduce onto the network or transmit data programmes, viruses and harmful software that is susceptible to causing damage to the access provider's computer system or their providers or third party users of the internet network.

Facebook, in its TOS (Terms Of Service) ascertains that the users accepts (amongst other things) to the following conditions when entering the social media:

- To not publish non-authorised commercial communications (like spam) on Facebook.

[4] Californian Penal Code, Section 502

- To not collect information or content from others users and to not access Facebook using automatic means (such as collection bots, robots, spiders or scrapers) without advance permission.
- To not upload viruses or any kind of malicious code.

7 The 7 Characteristics of Cyber-space

1. An environment where physical space and territory do not exist. Laws govern the earth, sea and air... space and the universe are not governed by current legal systems, and neither is cyber-space.

2. Time exists, but space does not.

3. A virtual world which is accessed by means of borders or ISPs and these computer tracks connect the two worlds.

4. An action on the internet can affect physical people and an action in the physical world can affect the virtual world.

5. In this world anti-social behaviours are born which cause harm to others (cyber-crimes, cyber-terrorism, cyber-privacy, virtual money without paying taxes...)

6. The following agents live alongside each other: cyber-organisations and cyber-citizens. States do not exist, although the USA, Israel and China are clear examples of States trying to forcefully "colonise" it.

7. The web is ideal to breach rules via the easy and cheap anonymity available.

8 Key Antisocial Behaviour on the Internet III

8.1 Spam

Spam is a quintessential element of the internet, a cyber-behaviour that is far from going away. As the years go by its presence is reinforced as it successfully overcomes the tools which try to get rid of the annoying messages that users are bombarded with on a daily basis.

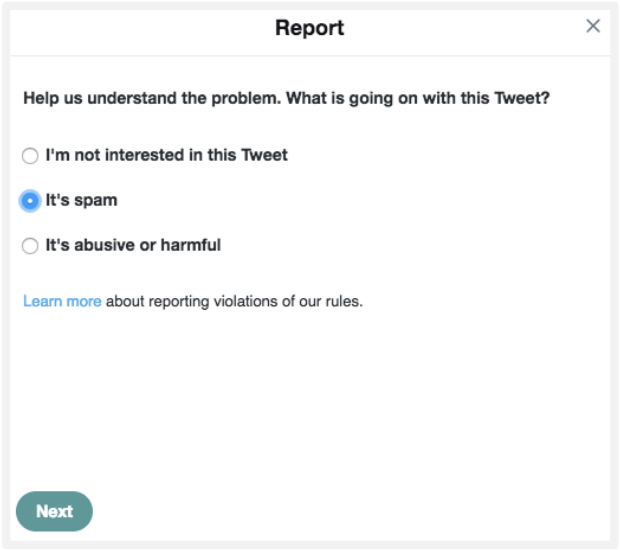
4.1.12.1 Scenario

SPAM refers to the unwanted, repetitive emails or messages (also known as junk mail) which have the main aim of publicising a product or service to somewhere that has not requested it or has any interest in it.

The action of sending unwanted emails is called *spamming*. Receiving these unwanted emails may just be a mere annoyance; although it may be a true problem when great volumes of them are received, creating a saturation of the services and, as a result, it obstructs the normal activity of the email service. Should this happen in a professional situation, this can even cause economical damage.

At times, these unwanted and repetitive emails may contain come kind of malware.

Another type of spam takes place on forums, chats and social media where messages are indiscriminately published advertising services or products; these can come to be quite annoying. However, as a general rule, this variety of spam is banned by the cyber-organisations in their terms and conditions of use. An example of this is Twitter:



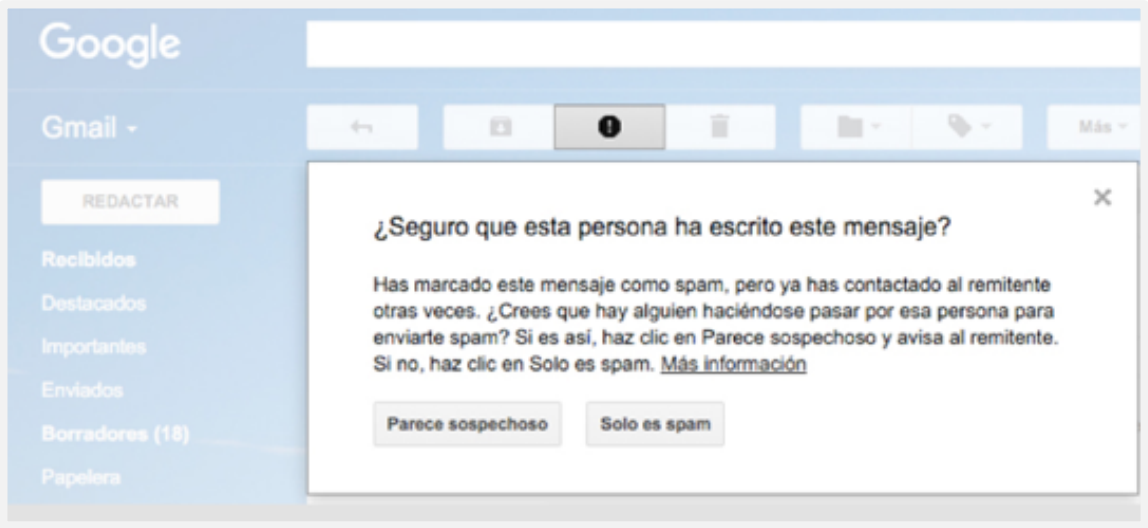
Example of reporting spam on Twitter.
Source: https://support.twitter.com/articles/365280

Instead of the classic method of this cyber-behaviour, dedicated to commercial promotion, it does not permit such an exhaustive control of the source of messages; albeit,

email providers such as Gmail and Hotmail are increasingly improving the scanners of this type of unwanted emails. And so, when they are detected, they are sent directly to the SPAM or Trash folders:

Example of spam on Gmail. Source: gmail.com

Additionally, on Gmail, if an email that has been received is spam it can be reported by using the following button:



Example of spam on Gmail. Source: gmail.com

Last of all, it is important to note that spam can come from any kind of user, be they individuals, companies dedicated to email marketing or infected computers.

12.2. Analysis

In the territorial world, spam is a conduct that has been thoroughly regulated in the majority of the countries analysed. This is not necessarily to the level that a specific regulation dedicated to spam would require, but it does fall within the Codes related to telecommunications and the internet.

For example, in **Spain**, sending commercial messages without previous consent is prohibited by Spanish legislation, both in Law 34/2002 on the Services of the Society of Information and in the Organic Law 15/1999 of 13 December on Data Protection. In this country, the sending of marketing or promotional communications by email or other equivalent means that have not been previously requested or authorised by the recipients is prohibited. This is apart from if there is a previous contractual relationship, providing that the lender legally obtains the recipient's contact details and they are used to send them marketing regarding the products or services of the lender's company that are similar to that which was initially procured by the client.

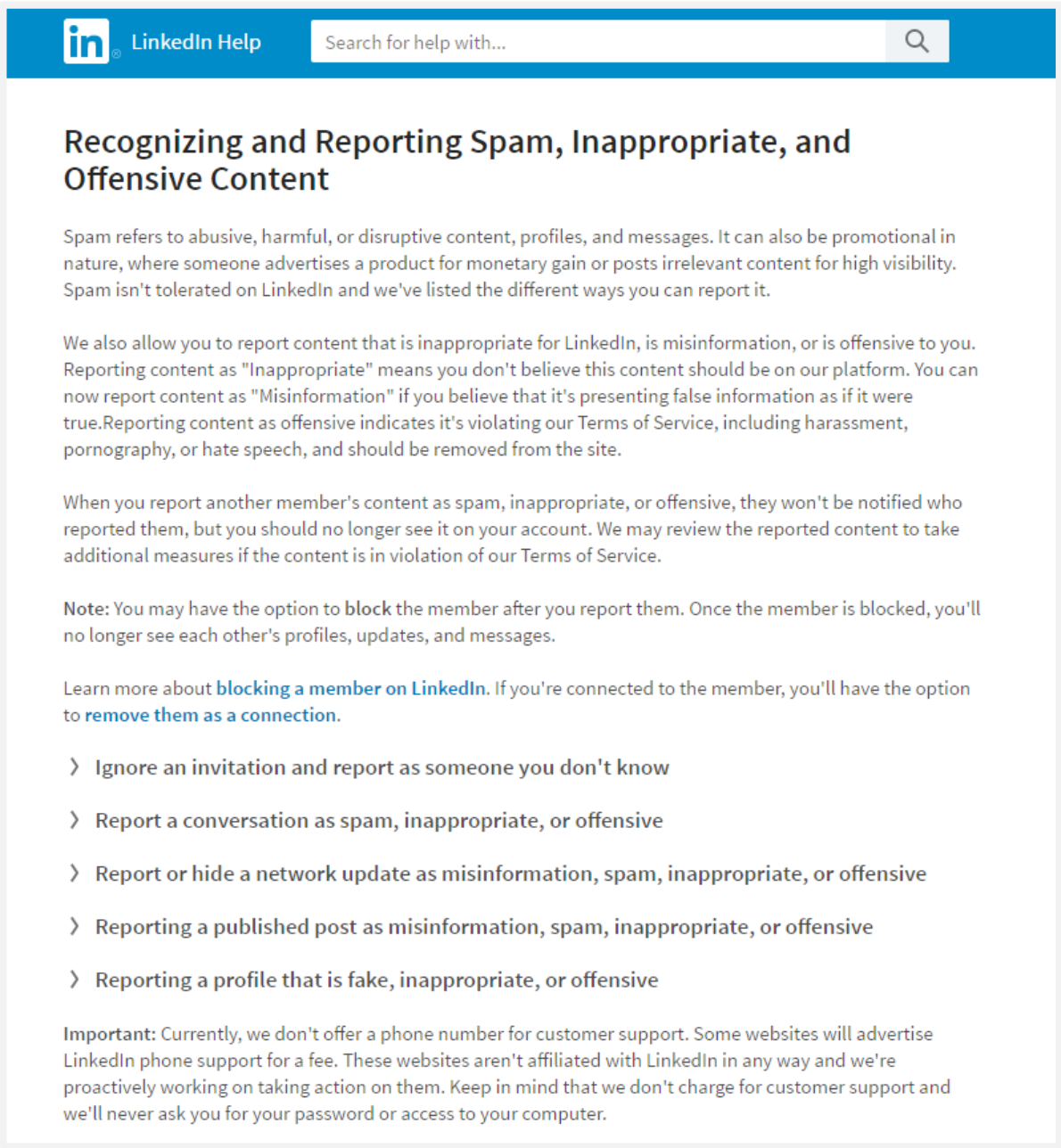
In terms of the USA, the **CAN-SPAM** Act (Controlling the Assault of Non-Solicited Pornography And Marketing **Act of** 2003) was passed. This legislation regulates the sending of commercial messages and emails giving those that receive them the possibility of opposing them and it lays down sanctions for those that do not adhere to the rules.

In **Chile**, law 19496 of 2 March 1997 obliges those that send promotional or marketing communications by email to indicate its subject matter in the "subject" section of the email, to identify the sender of the email and to state a valid email address to contact to request to stop receiving the emails. Anonymous emails and ones with incomplete information clearly infringe the law for Chilean institutions. If messages are sent after it has been requested that they are not, the sender can be penalised with a fine.

In cyber-world, spamming is one of the most regulated and delimited cyber-behaviours by all of the cyber-organisations.

For example the Terms and Conditions of **Linkedin** regulate spam and they prohibit it on repeated occasions. It also establishes that the users accept to fulfilling all of the relevant laws including, but not excluding others, anti-spam laws. Below is an outline of what users cannot do on the platform:

- Send spam and other unsolicited communications to other people.
- Publish unwanted and unauthorised advertising, promotional material, "junk mail", "spam", "chain mail", "pyramid schemes" and any other type of unauthorised advertisement.
- Interfere with the working or loading of the Services in an unreasonable way (such as spam, attacks via denial of service, viruses, game algorithms).

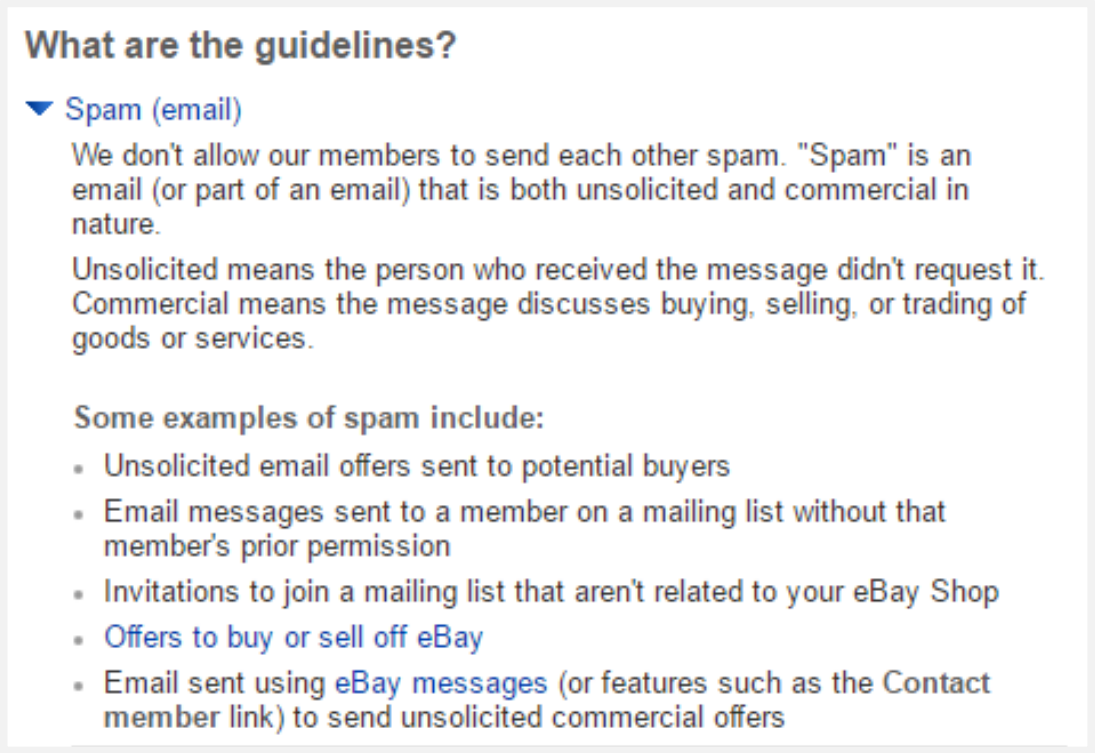


Example of the way LinkedIn helps with unwanted emails.
Source:https://www.linkedin.com/help/linkedin/answer/37854?lang=en

Pinterest is another example as its Terms of Service and Usage Policy prohibit spam, establishing that the user cannot try to interfere with any other Pinterest user, host or network, for example by sending viruses, overflowing the inbox, sending spam or with an excessive amount of messages. Likewise it is understood that should the user try to organise a competition or another type of promotion, they should not encourage **spam** by requesting, for example, that the participants write a comment.

In this section it makes sense to mention the figure of **Ebay**, due to its introduction of a different concept of spam compared to other organisations. Both in their Conditions of Use and in their content policies, the rules about spam are regulated and there is a strict policy about unsolicited commercial emails (spam). On Ebay unwanted emails are not

allowed to be sent to users to promote an item that is being sold on Ebay, or to seek an external, private transaction.
The site itself defines what spam is, defining it as unsolicited commercial email. They define unsolicited as a message that was sent to the recipient without their authorisation, and commercial as a message which is related to the sale of a product, service or promotion.



What are the guidelines?

▼ Spam (email)

We don't allow our members to send each other spam. "Spam" is an email (or part of an email) that is both unsolicited and commercial in nature.

Unsolicited means the person who received the message didn't request it. Commercial means the message discusses buying, selling, or trading of goods or services.

Some examples of spam include:

- Unsolicited email offers sent to potential buyers
- Email messages sent to a member on a mailing list without that member's prior permission
- Invitations to join a mailing list that aren't related to your eBay Shop
- Offers to buy or sell off eBay
- Email sent using eBay messages (or features such as the Contact member link) to send unsolicited commercial offers

Example of Ebay's anti-spam policy.
Source: http://pages.ebay.co.uk/help/policies/rfe-spam-ov.html

In the conditions of use, they state the duty to not distribute or send spam, bulk mail or unsolicited mail, chain mail or pyramid systems. And in the Policies, the general description makes a distinction about:

- The rules for everyone**:** They cannot improperly use Ebay's email forwarding system, nor can they send spam (unsolicited emails)

- The rules for adverts**:** As a rule of thumb, the sellers have to avoid using tactics such as the spam of key words as they difficult buyers' searches.

8.2 Cyber-extortion

Cyber-extortion is one of the most complicated conducts to combat given the nuances and levels of seriousness that it can adopt. As time has gone by, its importance has grown and right now it is rapidly expanding.

8.2.1.1 Scenario

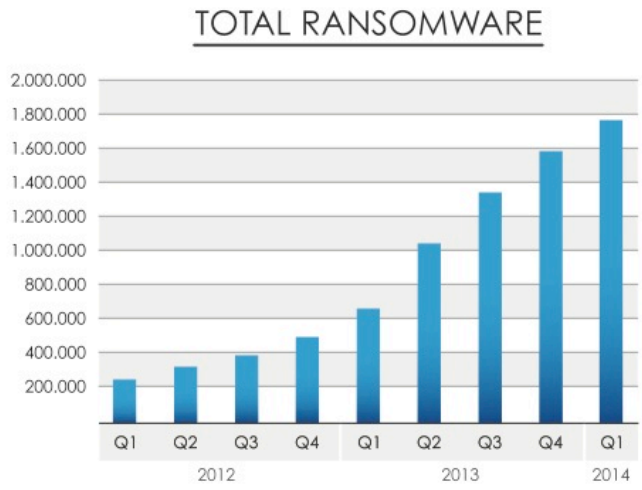
Extortion is the behaviour which obliges a person, by means of violence or intimidation, to carry out or omit some kind of act that is harmful to either themselves or others.

Normally these actions tend to have economical or financial objectives. The most frequent extortion scenario is blackmail and threats with the aim of receiving direct economical benefits from the extorted person.

On the internet, **cyber-extortion** consists of the same action: of using violence or intimidation, applied by means of computer mediums, in a way which gets the victim to carry out an action that is harmful to either themselves or others, with all the negotiations taking place on the web. The perpetrator and the victim do not have direct contact other than that which happens on the net.

The most common types of cyber-extortion are:

- The blocking of a personal computer, which is unblocked upon the receipt of an economic sum (ransomware).
- The access to mobile phones and smart phones being held hostage.
- The blocking of personal accounts on different social media.
- The threat of publishing information gathered about the victim.
- The sending of communications which threaten the recipient to hand over personal information.



Cyber-extortion is also formed of a subgroup of conducts which involve threats as the use of violence or intimidation towards people or things implies that the perpetrator threatens the victim; the taking over of information and documentation; fraud; and any other behaviour which may pressure the victim to then do something which harms either themselves or others.

What is strange about the most common form of cyber-extortion, the blocking of a device until money is paid, is that the amount asked for may seem very small and accessible, which means that, in the majority of cases, the victim pays. However, as a group, a network of extorted people may yield great benefits for the perpetrators. A clear example

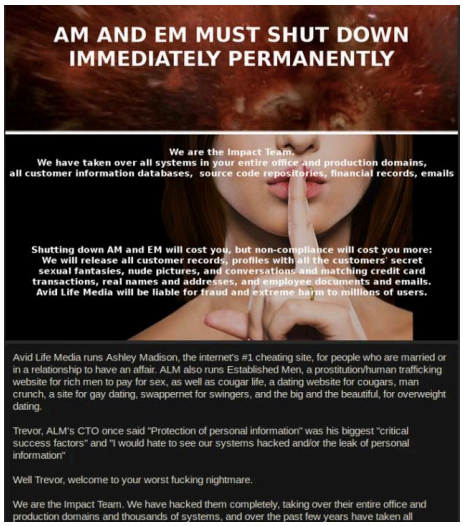
to illustrate this is who the use of Ransomware is able to be cyber-extorted, as for example the well-known Cryptolocker.

Screenshot of a Cryptolocker attack.
Source: Screeshot

In this regard, it must be noted that **there are no guarantees that if the victim adheres to the demands of the attacker, they will regain access to their device,** thus the accepting of their conditions does not guarantee the end of the attack.

Another form of cyber-extortion that is becoming more popular is the use of information that was filtrated on the web through hacking a database to request money in its exchange. This example can be found with what was happening with the attack on the Ashley Madison data bases.

DAILY NEWS 25/08/2015



Ever since a few weeks ago, there has been a topic on the lips of everyone in the cyber-space environment, it has provoked a range of different reactions and has even reached other parts of society. The Ashley Madison cyber-attack.

Ashley Madison is a dating and social media website for adults, aimed at encouraging persons either married or in a relationship to pursue an affair. It has around 40 million users worldwide.

What happened? In July a group of hackers called Impact Team accessed the Ashley Madison database, robbing hundreds of gigabytes about the organisation and conversations, addresses, photos and personal details about the users registered on the site.

Why? According to Impact Team, the attack is a way of getting back at the company for their bad entrepreneurial practices which include deceiving their users and the fact that there is only little security on their conversations. However, it is more likely that the motives were mainly economical as they also demanded the shutting down of the site in exchange for not published the stolen data.

What are the consequences? After the refusal to shut down the site, Impact Team released 10 gig of information which is now available to all internet users. This information is now being used by different cyber-criminals who are trying to extort those that are affected by the publication of said data.

Who is affected? The main victim is the Ashley Madison site, due to the loss of credibility, the advertisement of the serious security failures when storing information, and for deceiving users. But on the other hand, it is clear that the users whose personal details now appear on the web are affected, suffering from a range of attacks or having their bank details published and without them being able to take the information off the web.

Which measures are being taken? Currently, a reward is being offered for those people that provide information about the attackers' identities, or any other information that could help the investigation to progress. They are trying to get rid of the information that has been uploaded online, and institutions from each country are offering support to users that risk seeing their personal details published.

Without a doubt, this has been one of the most serious cyber-attacks and access to servers in recent years. But, compared to other similar events this has created a **cyber-extortion problem for the victims that affect them in cyber-space.**

In the physical world, extortion is the behaviour which obliges a person, by means of violence or intimidation, to carry out or omit some kind of act that is harmful to either themselves or others, usually of financial nature. But, on the internet, cyber-extortion consists of the same action: of using violence or intimidation, applied by means of computer mediums, in a way which gets the victim to carry out an

action that is harmful to either themselves or others, with all the negotiations taking place on the web. The perpetrator and the victim do not have direct contact other than that which happens on the net.

The most common forms of cyber-extortion include: the blocking of personal computers which are unblocked upon receipt of an economic sum, the access to mobile phones being held hostage and the blocking of personal accounts on social media and, in this case, the threat of publishing the information that has been collected about the victim.

Cyber-extortion poses a difficulty that is seen in other cyber-behaviours that are found on the internet: It is a cyber-problem that affects people in cyber-space, therefore there is not an applicable legal system, nor an appropriate court to judge the acts that have been committed. Cyber-crimes are not committed in a clear, territorial location, therefore current legal systems cannot act efficiently.

Cyber-extortion may be prosecutable within legal systems where the place that the crime was committed can be identified, as well as the perpetrator. That is the case with Spain, where it is prosecutable with prison sentences of 1 to 5 years, through the crime about extortion in section 243 of the Criminal Code. But without a doubt, as a cyber-behaviour certain territorial barriers that condition legal systems to be applicable in a concrete place marked by physical borders will have to be overcome.

8.2.1.2 Analysis

From a territorial perspective, cyber-extortion is present in the Criminal Code of all the territories analysed, it forms part of a group of crimes that do not require a specific, exclusive regulation, but they are important enough to always be addressed.

In **Argentina**, the cyber-extortion has be prosecuted under sections 168 to 171 of the Criminal Code with regards to extortion. The basic behaviour consists of intimidation or the simulation of a public authority, forcing somebody to hand over, send, deposit or make available to a third party, items, money and legally binding documents. In terms of the sentence, terms of detention or imprisonment of between 5 to 10 years are enforced. Likewise, in the majority of territories it is envisaged that these crimes are committed by individuals in their own private field. Section 169 states that anyone who threatens the honour of another or threatens to violate their secrets, in exchange for one of the things mentioned above, will be reprimanded with prison sentences of between 3 to 8 years.

Another example is that of **Bolivia**, which can legally prosecute cyber-extortion thanks to section 333. Anyone who, by means of intimidation or serious threat, compels another to do something, tolerate something or stop doing something, with the aim of gaining an advantage or economic benefit for him/herself or a third person, will be punished. The sentence is a prison term of 2 to 6 years.

Something similar happens in **Spain;** section 234 of the Criminal Code condemns anyone who, for a profit, uses violence or intimidation to force somebody to carry out, or not carry out, an action which may harm them or a third party. In this case, the prison sentence is between one to five years.

The treatment of this behaviour in cyberspace is not explicit, but it is addressed through the behaviour that can make up part of cyber-extortion. On **Badoo**, the terms and conditions establish that content cannot be published if it is :

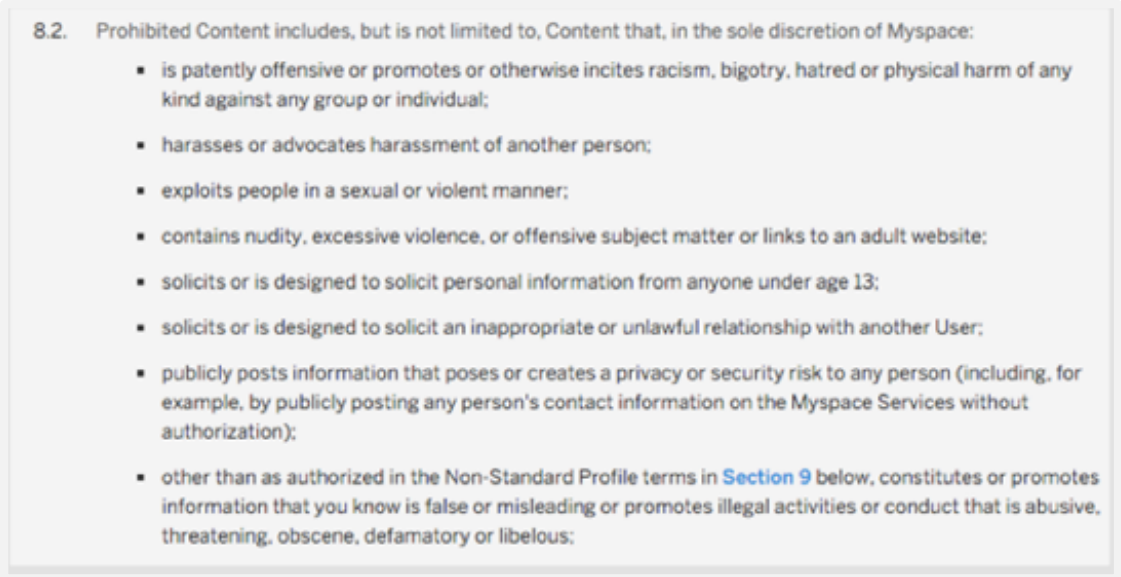
1. Abusive
2. Insulting
3. Threatening
4. Promotes racism, sexism, hate or intolerance

Following the same example, the Terms and Conditions of **Twitter** and their Rules of Use do not permit the following in relation to cyber-extortion:

- **Violence and threats**: the user cannot publish or send threats of direct or specific violence against others.
- **Illegal use**: the user cannot use out service for any illicit means or to promote illegal activities. International users accept to adhere to the local laws referring to any online behaviour and acceptable content.
- **Directed abuse**: The user cannot direct any abuse or harassment.

As a final example, we can look at the Terms and Conditions of **Myspace**, which establish that users cannot:

- Upload content that is clearly offensive, promotes violence or incites racism, hate or violence towards a certain group or individuals.
- Upload content that is abusive or promotes abuse towards another person.
- Publish information that could create a security or privacy problem for somebody.
- Upload false content or content that promotes illegal, aggressive or defamatory activities or conducts.



8.2. Prohibited Content includes, but is not limited to, Content that, in the sole discretion of Myspace:

- is patently offensive or promotes or otherwise incites racism, bigotry, hatred or physical harm of any kind against any group or individual;
- harasses or advocates harassment of another person;
- exploits people in a sexual or violent manner;
- contains nudity, excessive violence, or offensive subject matter or links to an adult website;
- solicits or is designed to solicit personal information from anyone under age 13;
- solicits or is designed to solicit an inappropriate or unlawful relationship with another User;
- publicly posts information that poses or creates a privacy or security risk to any person (including, for example, by publicly posting any person's contact information on the Myspace Services without authorization);
- other than as authorized in the Non-Standard Profile terms in Section 9 below, constitutes or promotes information that you know is false or misleading or promotes illegal activities or conduct that is abusive, threatening, obscene, defamatory or libelous;

Example of Myspace's abusive behavior policy.
Source:https://myspace.com/pages/terms#8

8.3 Threats

With the complete dominance that social media has in the ecosystem of the internet, it is inevitable that they are home to one of the cyber-behaviours that are most frequently backed up by anonymity and distance: threats.

8.3.1.1 Scenario

Threats are defined in the physical world as "intimidating somebody by advertising the provocation of serious harm to him/her or their family". In the majority of case these are expressed either verbally or by some form of writing.

On the internet, this behaviour can be defined in the same way. **Cyber-threats** are understood as using the web, smart phones or other electronic technology to intimidate another with the advertising of the provocation of serious harm to him/her or their family.

In a broad sense, this behaviour also includes insults, harassments and intimidations. Cyber-threats tend to go hand-in-hand with cyber-extortions and cyber-bullying situations. For that reason, often these behaviours that can be individually identified are grouped together as one.

Cyber-threats, just like threats in the territorial world, do not have to be exclusively directed towards the person being threatened, but they can fall on their close friends, relatives or partners.

Example of cyber-threats on Twitter.
Source: twitter.com

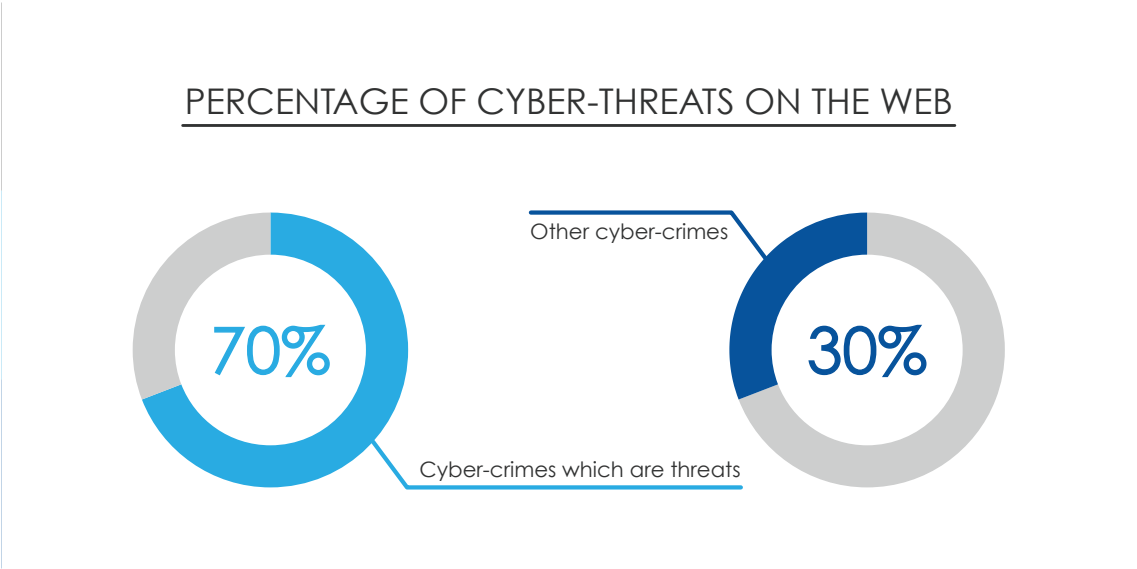
With regards to the channel of communication, this can be any channel that is available in the cyber-world, from instant messages to emails, forum and blog publications or conversations on online video games.

In terms of what the victim is threatened with, it has to be believable, whether it is a crime or not, and it must take note of the context and situation in which it was made, as it will

not always be taken in the same way. A threat between two school children in the playground is not the same as a threat at work between two co-workers.

As for who can fall victim to these threats, most commonly it happens between natural persons, however it is possible to find threats which come from the spokesperson of a group, in representation of all its members, against other groups or individuals, such as those made by the representatives of determined organisations. However, these two last cases are less common, as threats tend to be personal and individual.

To paint a picture of the magnitude of this behaviour, according to the Spanish Ministry for Home Affairs Statistical Yearbook, in 2011, 9,839 threats were made over the internet, 9,207 in 2012, 9,064 in 2013 and 9,559 in 2014. Furthermore, this study warns that threats make up 20% of the crimes that happen on the internet.



8.3.1.2 Analysis

In general, the use of threats in the physical world is regulated by the different Criminal Codes and sentences oscillate between 8 months and 8 years of imprisonment.

The basic behaviour is categorised within the Criminal Codes, as there are no specific laws or codes solely dedicated to threats, which are the act of "warning another person that serious harm will happen to that person or their loved ones".

The majority of legislations coincide by giving lower sentences for threats that do not go with any kind of condition.

However, this sentence tends to be greater should it be accompanied by the following circumstances:

- A quantity of money is demanded when making the threat
- Weapons are used when making the threat
- Two or more people take part in the threat making
- The threat is followed with a condition
- It consists in causing terror to the population

- The threat is made anonymously
- The threat forces another person to commit a crime
- The perpetrator of the threat is in disguise

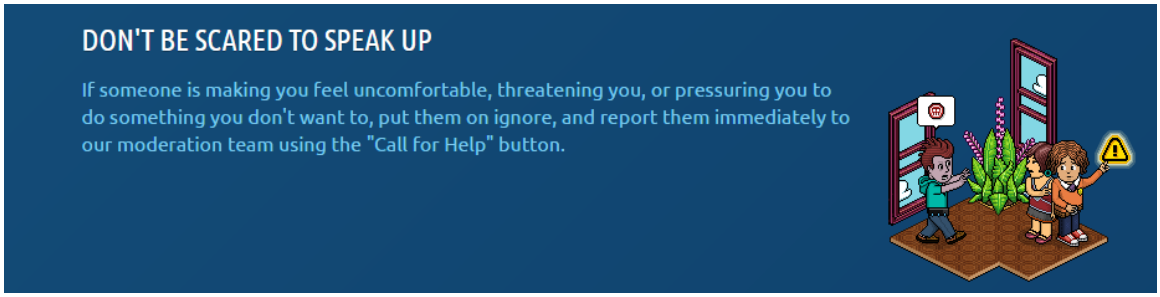
However, it is a very variable crime in terms of the circumstances, the means by which it can be committed and the regularity or seriousness of the insults. Therefore, clear rules which are equal across legislations cannot be established in terms of its treatment or sentences.

In cyber-space, there are also rules which regulate the use of threats and generally, these are found with the organisations' Terms and Conditions of use.

As has been already discussed, social media are the organisations where this cyber-behaviour most commonly takes place, and because of this the use of threats is prohibited in all of their conditions of use. For example, on **Facebook**, their community rules make reference to threats and states that:

- Should a direct threat to public security be made, Facebook will delete the content and may get in contact with the security forces.
- Threats of violence towards people or the organisation are not permitted.
- Organisations that are involved in terrorism or criminal acts of violence are not allowed to be present on Facebook.

Likewise, in the Terms and Conditions of the social network **Habbo**, the following are prohibited: slander, abuse, harassment, bullying and threatening or violating in any other way the rights of other people. They also encourage their users to report inappropriate content.



Example of support on Habbo.
Source: https://www.habbo.com/playing-habbo/safety

Google+ also prohibits this behaviour, it establishes that users must not: slander third parties, commit abusive acts against them or harass them,
stalk them, threaten them, or infringe their legal rights at all in any way.

The efforts that all the organisations make in terms of regulating the problem of threats is noteworthy, in practice all of them have a button that can be used to report threats and they can be analysed with the intention of deleting the user that sent them.

8.3.1.3 Proposed solutions

The answer to the act of threatening by electronic means, via cyber-space, has always been articulated under the initiative of the cyber-citizens, in this case addressing the key people implicated and the protagonists of these actions.

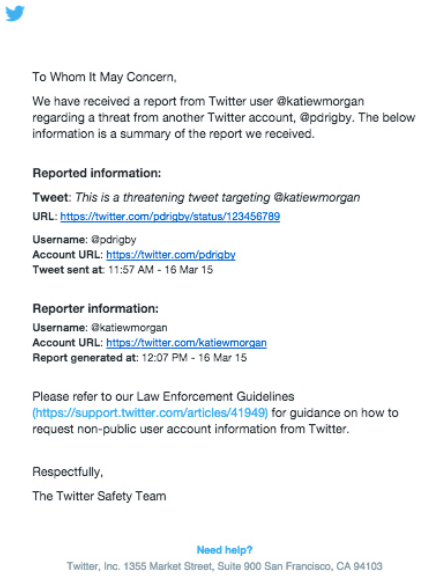
Passing the power to the cyber-organisations to manage the freedom of speech from the first moment on the internet cannot be the solution to cyber-threats.

Likewise, it is not possible to demand the creation of a list of catalogue to process the perpetrators automatic deletion (as is the case with banned or blocked terms), given that cyber-threats will continue to be made via other channels or with other vocabulary, as is currently the case.

The improvement of the implementation of the mechanisms to report threats (reactive and proactive mechanisms) should be advocated. This, together with specific and detailed policies regarding the prohibited behaviours in each cyber-organisation, will allow for a more efficient deletion of the users that commit these crimes than currently exists.

Likewise, and in second place, these cyber-users can turn to the cyber-representation of the Security Forces of the State Security, which after the filtering from the cyber-organisations, will be able to provide solutions to those that request the prosecution and deletion of the cyber-threats.

DAILY NEWS 18/03/2015



To Whom It May Concern,

We have received a report from Twitter user @katiewmorgan regarding a threat from another Twitter account, @pdrigby. The below information is a summary of the report we received.

Reported information:

Tweet: *This is a threatening tweet targeting @katiewmorgan*
URL: https://twitter.com/pdrigby/status/123456789

Username: @pdrigby
Account URL: https://twitter.com/pdrigby
Tweet sent at: 11:57 AM - 16 Mar 15

Reporter information:
Username: @katiewmorgan
Account URL: https://twitter.com/katiewmorgan
Report generated at: 12:07 PM - 16 Mar 15

Please refer to our Law Enforcement Guidelines (https://support.twitter.com/articles/41949) for guidance on how to request non-public user account information from Twitter.

Respectfully,

The Twitter Safety Team

Need help?
Twitter, Inc. 1355 Market Street, Suite 900 San Francisco, CA 94103

The social network Twitter has just announced a new measure against the crime of threatening via the Internet. The user's security manager, Ethan Avey, announced in his blog yesterday that from now, the user that reports another for a tweet that could be considered as threatening or offensive will see a button on their Twitter account which allows them the receive a written report about the complaint.
The content of this report will include:

1. The content of the tweet that was reported
2. Its URL
3. The name of the user and author of the tweet
4. A link to their profile
5. The date that the tweet was published and the date that the complaint was made
6. The details of the person that reported the tweet.

This measure aims at becoming a support for the decision making in terms of whether or not to take legal action. However, what is most interesting about this is the possibility that it gives the complainant the chance to see when the "hate" tweet was sent, should the perpetrator have decided to delete it. Even so, Twitter recommends to always contact the appropriate authorities in cases where the physical integrity of a person is at risk.

8.4 Identity theft

The phenomenon of identity theft is a problem that can appear in all areas of cyber-space, whilst also affecting those areas in the physical world which are vital for individuals. This behaviour is one of the most harmful that is currently in existence.

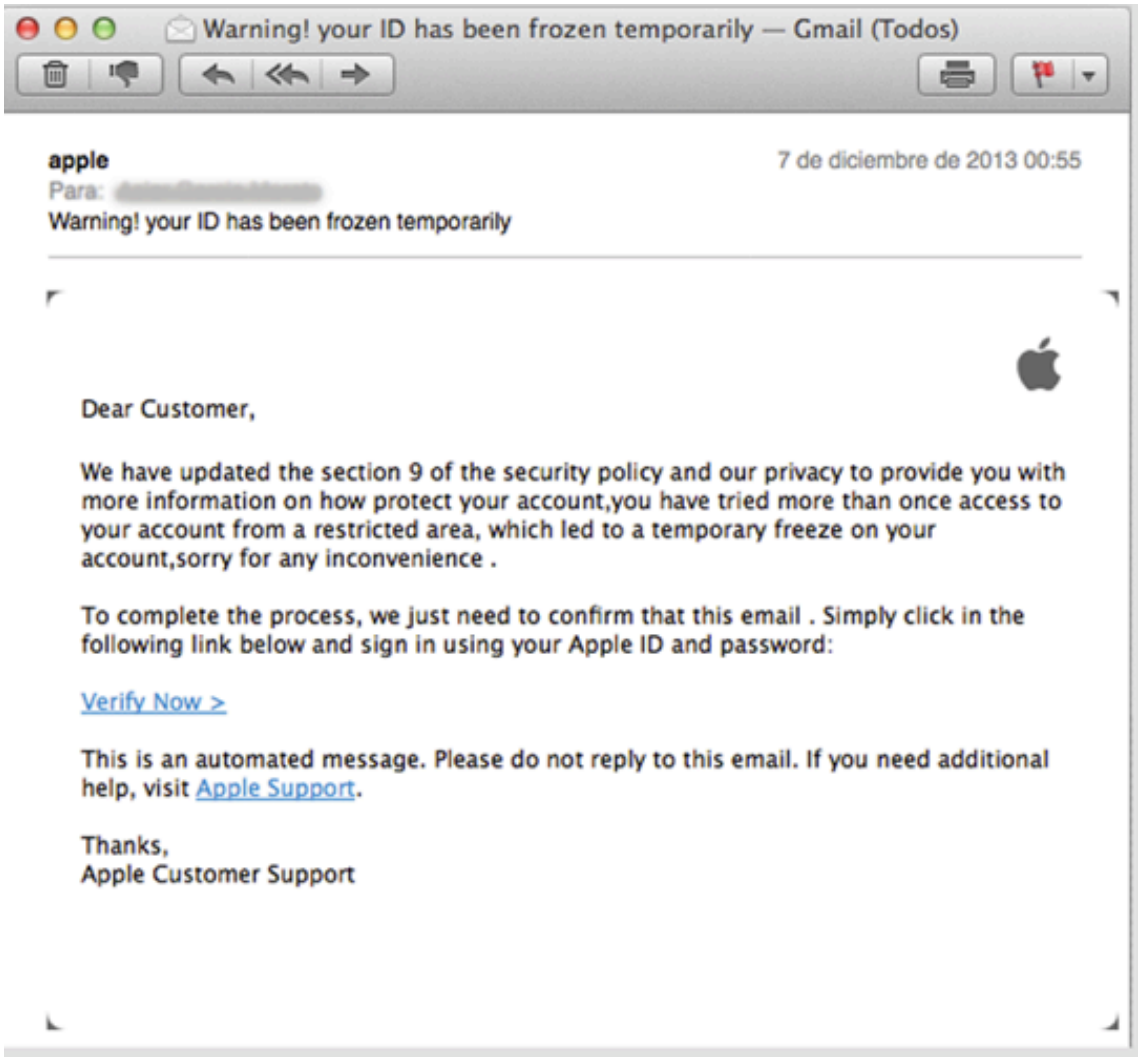
8.4.1.1 Concept

Identity theft, in the territorial world is a behaviour which involves the appropriation of another person's identity or the usurpation of their civil state.

On the internet, this involves stealing someone's identity, this occurs when somebody uses another person's name or photo etc. In fact, it can be anything that digitally identifies the other person, with the aim of self-benefit or of causing harm to the true holder of the identity in question.

The methods of identity theft are multiple and varied, but these are the most common:

- Phishing: is the technique by which the perpetrator tries to simulate that a web page (which is in reality a fraud) is the original and true page (for example, a bank's website), with the end goal of obtaining confidential personal details to subsequently use them for malicious means. Generally speaking, the phishing techniques tend to make use of emails as a tool: the potential victim receives an email which, on the service, seems to be from a known company which they trust. Said email asks the victim to click on a link to change their access codes because their account had been in a compromising situation, for example, or for any justifiable reason that seems legitimate.



Example of phishing.
Source: Apple's email service

- Scam: makes reference to any kind of attempt of fraud by means of any internet media, such as emails or fraudulent web pages.
- Spoofing: makes reference to the use of technique by which an attacker, normally with malicious uses, makes out that they are a distinct entity by means of the falsifying of data in a communication.
- Forging of cyber-documents.
- Social engineering: by using this technique, a person can pass themselves off as another, with the aim of obtaining certain, generally confidential, information.

8.4.1.2 Analysis

In the territorial world, very different regulations can be found regarding the same problem. This is due to the notable difference of the concept of identity theft found in the countries analysed.

In the **United States,** identity theft is regulated in the "Identity Theft And Assumption Deterrence Act" of 1998 which came in to introduce amendments to chapter 47 of title 18 of the "United States Code" regarding identity fraud, making identity theft a federal crime which leads with it prison sentences of up to 15 years and fines of up to 250,000 dollars. It does also consider identity theft both in the cyber-world as well as in the physical world.

In **Puerto Rico**, identity theft is considered as the strictest sense of the crimes that make up identity theft. Thus, it includes the conducts that people carry out with the aim of being fraudulent, and by means of whatever manipulation of information, they achieve the non-consented transfer of any asset or patrimonial right which harms either a third part or the State. The sentence that the Criminal Code outlines is a fixed prison term of 8 years.

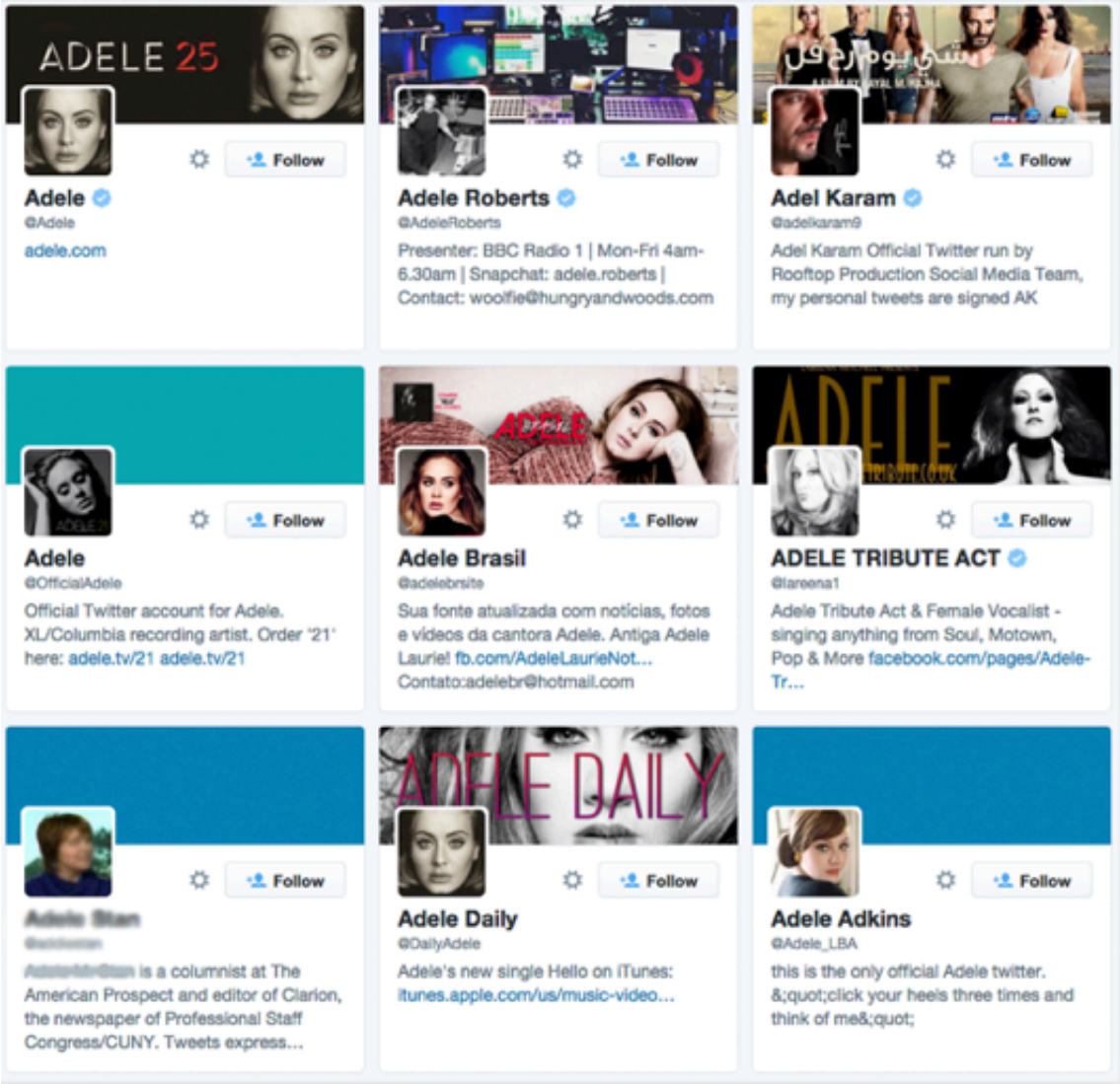
In Spain, a heterogeneous concept of identity theft can be found. The Criminal Code considers identity theft as a crime, defining it as the usurpation of a civil state. Section **401 penalises anyone who** usurps the civil state of another with prison sentences of between 6 months to 3 years. However, for the identity theft to be considered as such, the individual who usurps the civil state of another has to do so for a continued amount of time, something which does not always happen. It is because of this that, on many occasions, identity theft tends to be recognised as something else like, for example, depending on the circumstances, fraud.

In the world of cyber-space, the cyber-organisations that consider the problem of identity theft expressly permit it, without leaving any room for interpretations or loopholes about the validity, or lack of, of this behaviour. However, unless the person affected or their acquaintances do so, this cyber-conduct is rather difficult to detect when it comes to anonymous or not very well known individuals.

This does not mean to say that it does not happen; on the contrary, often cyber-criminal create these kind of anonymous identities so as to more easily pass under the radar of the rest of the users.

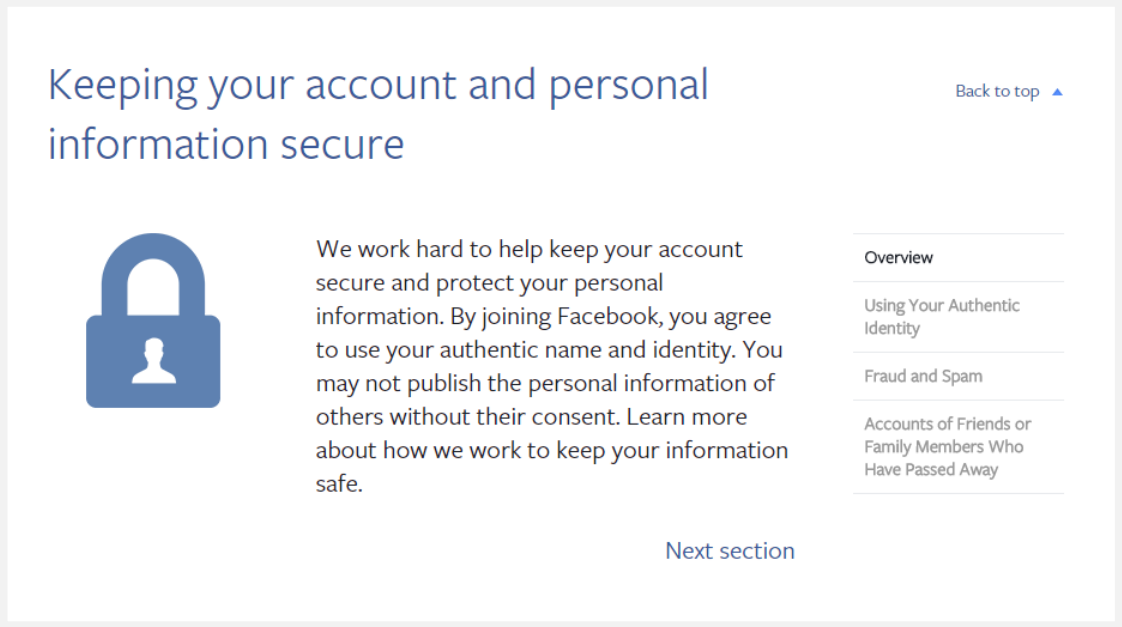
On social media it is common to find a far more exact control of the accounts that impersonate public figures, as well as those well-known organisations or companies with an already existing profile on the internet.

For example, Twitter uses a blue tick to verify the authentic accounts of people and companies that have an impact on society:



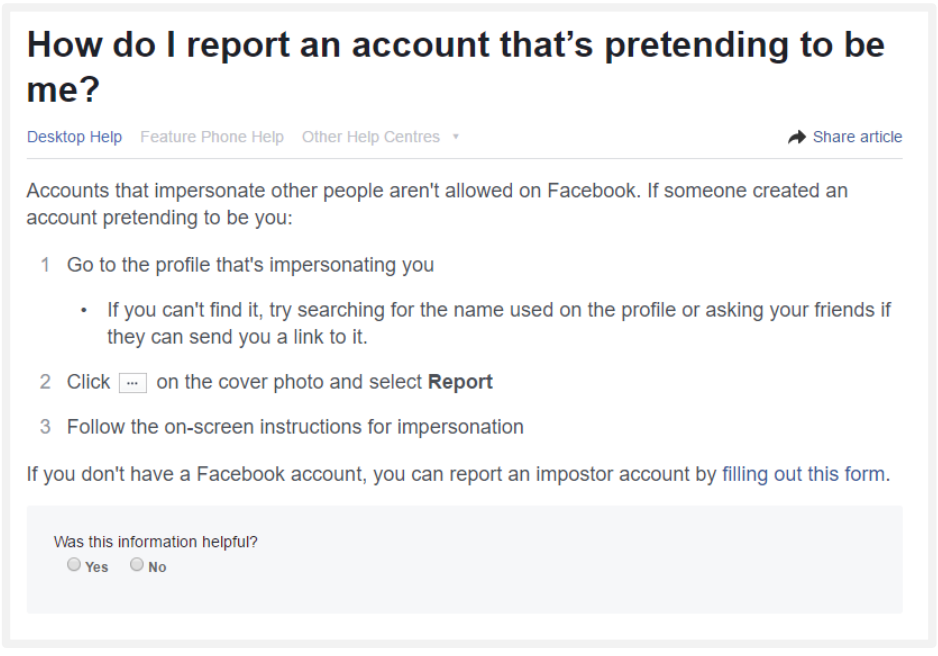
Example of identity theft on Twitter.
Source: twitter.com

Facebook is amongst those organisations that regulate identity theft. This platform only allows users to register with their real identity, should they use another identity or have various profiles, Facebook reserves the right to close them.



Form to report identity theft on Facebook. Source: https://www.facebook.com/communitystandards

Moreover, complimentary to what was previously mentioned, they have a mechanism for reporting fake profiles:



Form to report identity theft on Facebook
Source: https://www.facebook.com/help/174210519303259

Another example can be found on **Amazon**, where, once again, identity theft is expressly prohibited, without the scope for possible interpretations. Their Terms and Conditions state that "false email address cannot be used", "you cannot steal the identity of another

person or entity" and you cannot even "falsify the origin of contents in any way", meaning that identity theft is prohibited in this organisation.

What would be particularly recommendable to delimit how this ever more common cyber-problem spreads, would be to introduce mechanisms on the distinct platforms that make up cyber-space to report such issues and to introduce some brief, simple and efficient procedures to combat them.

8.5 Cyber-bullying

Currently, with the proliferation of minors using the internet, who use it more than any other group of users, cyber-bullying is one of the behaviours that they most suffer from, but also that they most carry out.

8.5.1.1 Concept

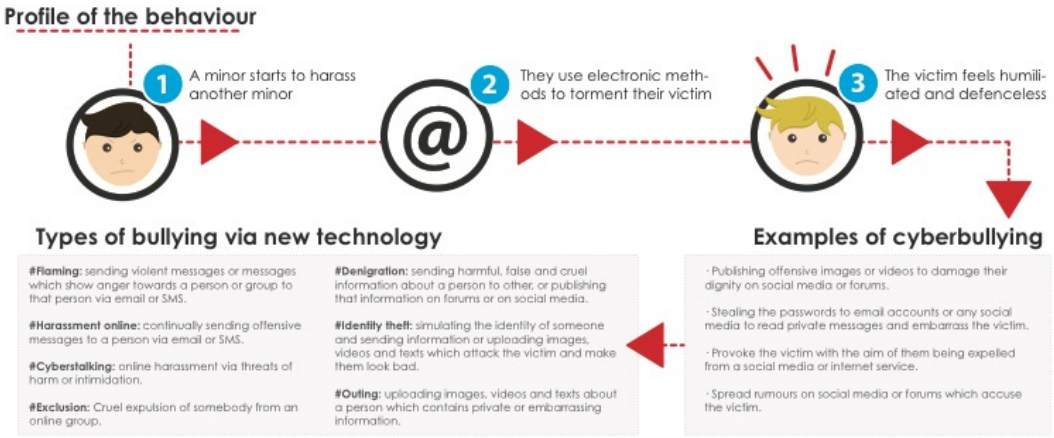
Without going into too much detail, and for didactic purposes, bullying can be defined as the behaviour whereby some minors decide to annoy younger or more vulnerable minors by means of harassment, threats, extortions, etc.

This is generally aimed at those who are different, that do not wear fashionable clothes or that form part of a social or ethnic minority. It also often happens due to physical defects, being overweight, clumsiness or even for being studious or shy.

The intention of this activity is to hurt, humiliate or leave a person out of a circle of friends or of a specific community. However, it is possible that many children carry out these acts simply because the other child already suffers from this abuse from other classmates or friends.

On the internet this behaviour, which can be called cyber-bullying, occurs when someone who is under-age torments, harasses or humiliates another by means of the internet, smart phones or another electronic technology.

Children must be both the perpetrators and victims of this attack for it to be considered cyber-bullying: if there is an adult involved it is a case of cyber-harassment.



According to a study carried out by ESET in Latin America in 2013, it is estimated that 30.7% of young people have been harassed via some form of electronic device. In this regard, this study confirms that 8 out of every 10 teenagers that were affected by bullying to not ask for help or tell their families or authorities about what was happening.

This activity is currently one of the most worrying threats as it severely affects development during adolescence and youth, it can even so as far as to lead to isolated cases of suicide due to the discrimination, isolation and threats that the victims of cyber-bullying suffer from.

The most common types of cyber-bullying on the internet are:

- Those that coincide with cyber-harassment such as registering the victim on different websites, creating false profiles and imitating the victim's identity and publishing information which harms their dignity.
- Robbing the password to an email account or social media profile in order to read private messages and passing themselves off as the victim by sending false and/or sensitive information to their contacts and thus embarrassing them.
- Provoking the victim to react in a violent way on an internet platform with the aim of getting them expelled by it moderator.
- Spreading rumours on social media or on forums which accuse the victim of carrying out a condemnable conduct, in such a way that others, without doubting what they read, carry out their own forms of reprisal or bullying.
- Threatening via email, SMS messages or on social media

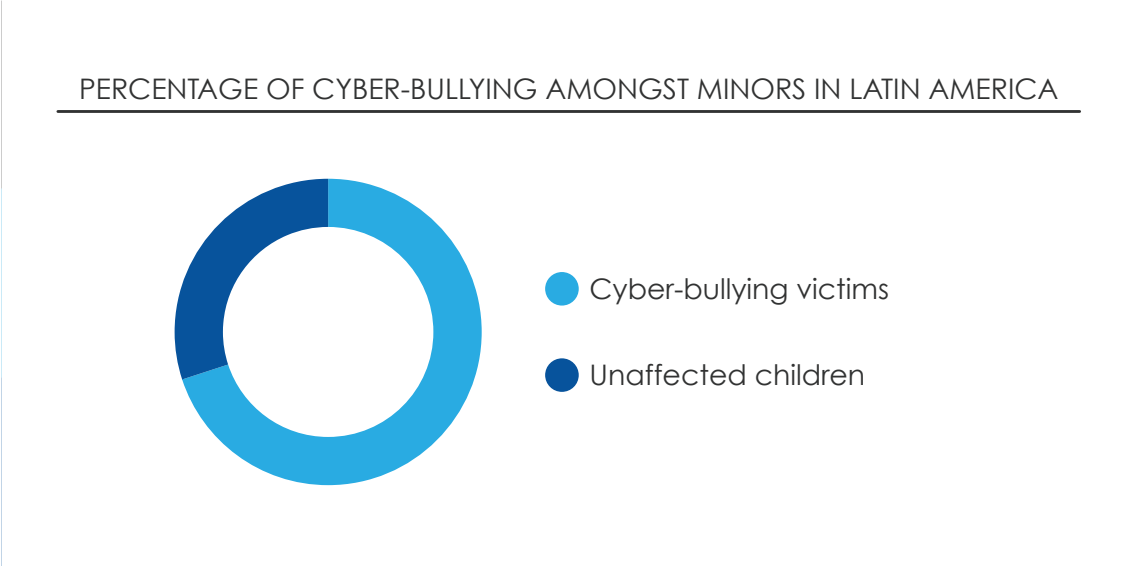
These definitions can be dealt with by identifying seven categories of verbal and written harassment via new technologies:

1. Flaming: The sending, via email or SMS, of violent messages to an individual which show anger towards that person or a group.
2. Online harassment: The continual sending of offensive messages to an individual via email or SMS.

3. Cyber-stalking: Online harassment by means of threats of physical harm or intimidation.
4. Belittling: The sending of prejudice, false and cruel information about a person to another, or the publication of this information in forums or on social media.
5. Impersonating the person: Taking on the identity of a person and sending information or uploading images and texts which attack and make the victim look bad.
6. Outing: The uploading of videos of text about a person which contain private or embarrassing information.
7. Exclusion: The expelling of a user from an online group formed on some kind of platform.

8.5.1.2 Analysis

According to a study carried out by the NGO Plan Internacional, Latin America is the region with the world's highest rate of cases of bullying, with some 70% of children falling victim to this conduct. Colombia leads the pack, with 20% of all children in this country being victims of bullying.



Bulling is **not classified in any Criminal Code** in Latin America or Spain. However, it could be constitutive of a crime of:

a. Threats
b. Coercion
c. Slander
d. Harassment

In other words, for this behaviour to be classed as a crime, it must be included within one of the above-mentioned crimes.

As a general rule, the following distinction is made:

- If the crime is committed by someone under 14 years of age: the minor will not be judged or declared criminally responsible, in that sense prison sentences cannot be applied. However, measures will be taken to verify the guarantee of rights and

to re-establish links to the education process. In other words, the school will be informed of the events so that that can take measures to protect the victim.

- If the crime is committed by someone between 14 and 18 years or age: the Criminal code does play a part and the minor may be confirmed criminally responsible and their freedom may be deprived as a pedagogical measure. The events will be judged in line with each country's respective Criminal Code (should the cyber-bullying be considered as a crime of slander, threats, coercion or harassment) providing that that events are sufficient enough: there must be an action (degrading treatment) and a result (damage to moral integrity).

In additional to what has been mentioned, cyber-bullying also involves a civil responsibility, meaning that compensation must be paid due to the harm caused to the victim. The harm or damaged caused may be patrimonial (harm caused and losses) or extra patrimonial (moral damage).

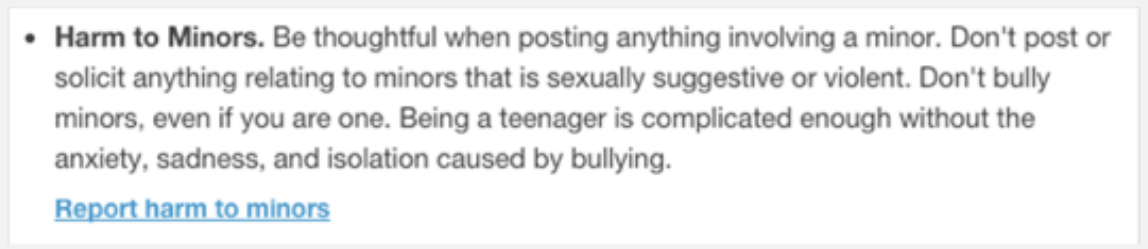
In cyber-space there are is a scope of rules that indirectly penalise Cyber-bullying. For example, the conditions of use of **Myspace** state, in their eight paragraph, that the following are not permitted to be uploaded by users:

- Content that is clearly offensive, promotes violence or incites racism, hate or violence towards a certain group or individuals.
- Content that is abusive or promotes abuse towards another person.
- Content that sexually or violently exploits people
- Content that is excessively violent or is offensive
- Content that requests the personal information of anyone under the age of 13 years.
- Content that requests, or thinks to request, inappropriate or illegal relations with other people.
- Content that could create a security or privacy problem for somebody.
- False content or content that promotes illegal, aggressive or defamatory activities or conducts.

Tumblr also prohibits the following related conducts in their Terms and Conditions:

- Encouraging self-destructive behaviour
- Encouraging harm to minors
- Promoting violence or hate towards others on the basis of intolerance
- Harassing other users
- Removed invasion of privacy
- Uploading illegal content or uses Tumblr for illegal means

In summary, all organisations indirectly prohibit cyber-bullying by regulating all types of behaviour which is threatening, harassing, encourages violence and invades privates, etc.



Screenshot of Tumblr's Terms and Conditions.
Source: tumblr.com

8.5.1.3 Proposed solutions

The solution to cyber-bullying has to come in an array of measures which are implemented by the parents of the perpetrator and the tutors of the victims, as well as those subjects who are directly affected. This is a problem which requires efficient measures from the get-go which work as much so as a preventative measure as in an immediate way.

- Every message or photo which is uploaded to social media that involves bullying must be reported.
- New email accounts should be made, as well as the accounts of other organisations through which this behaviour is carried out.
- Access should be restricted to open social media profiles.
- And last of all, offensive material on the web must be deleted, in application of the right to be forgotten.

Likewise, in terms of the physical world, the Security Forces in each State must always be contacted to report this kind of behaviour. And measures, similar to those set out for cyber-space, should be applied, or mechanisms that are available in the victim's school environment should be used.

8.6 Bank Fraud. Phishing, Pharming.

On 23rd November 2015, the Spanish National Cyber-Security Institute (INCIBE), by means of their Internet User Security Office (OSI), once again issued a warning about a new case of phishing. In this case, the attack tried to steal the data of the coordinates card of La Caixa, as the following extract explains:

DAILY NEWS 23/11/2015

They tried to steal your La Caixa coordinates

A new attempt was made at stealing the security data of online banking users, this time by trying to obtain the data of the coordinates cards of the La Caixa online bank by means of a phishing procedure in which a web page simulated the La Caixa page.

The fraudulent web page which tried to steal the data from the coordinates cards on La Caixa users has been housed in a hacked web page in Holland. http://badmintonsale.nl/js/2016/security-suXX16/client.htm.

In this web page, the colours and logo of La Caixa were imitated, and then users were requested to introduce the number of their Online Banking coordinates card, as well as the numbers of the coordinates positions which come on the card.

The aim of this new fraud is to obtain the private coordinates of individual users of La Caixa's online banking, to then use this data with malicious aims.

Bank fraud carried out via phishing or pharming mechanisms is one of the most widely spread conducts in cyber-world. To fight this, prevention and attack measures are constantly being carried out. However, what is true is that despite the improvements in security measures, there are still internet users who continue to fall into this kind of trap.

Computer-related fraud in Spain (according to the Ministry for Home Affairs)			
2011	2012	2013	2014
21.075	27.231	26.664	32.842

8.6.1.1 Scenario

Bank fraud on the internet is as a result of diverse techniques, and phishing and pharming are found among those. It must be highlighted that despite the fact that phishing and pharming techniques are mainly used to carry out bank frauds, they can be used to deceive the user in any other area, not just in terms of banking.

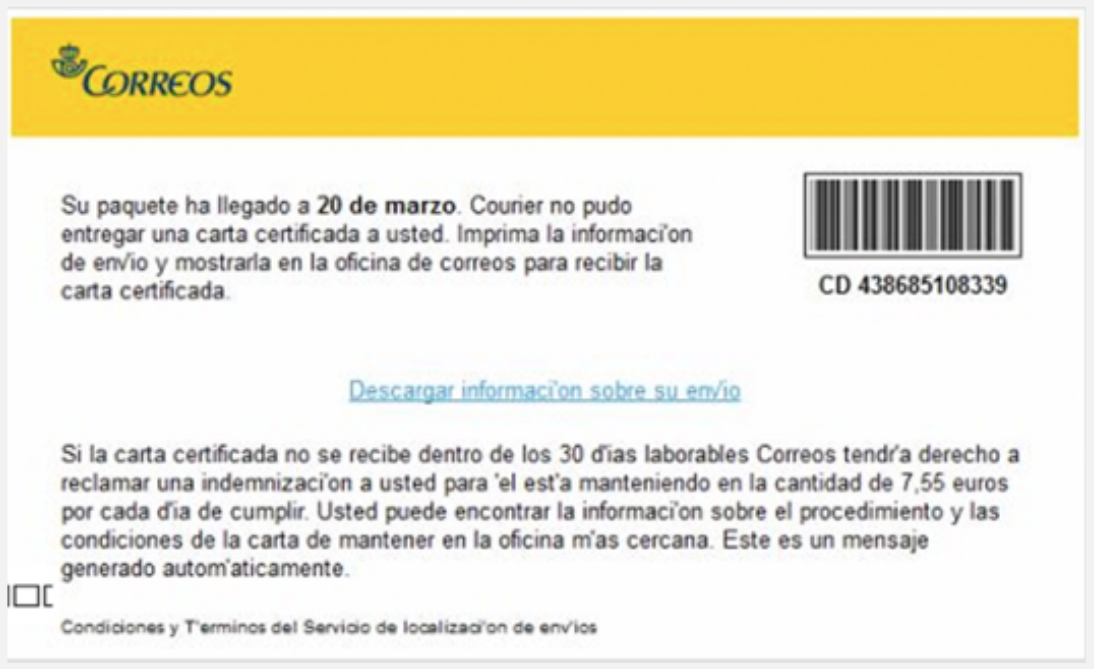
- **Phishing** involves the sending of web links, making them available to users, using the different ways available on the internet (normally via email or web pages). Through this, individuals are directed to click on said link which takes them to pages which try to obtain their confidential data by means of deceit.

Both the links and the web pages that the internet user is led to appear to come from reliable sources, such as trustworthy people, companies or bodies with whom the user already has a relationship. This way, the user believes that they are surfing on a completely safe site, and they enter the information that is asked for; this allows the cyber-criminal to obtain personal data (passwords, personal details, bank information, etc.) directly from the tricked user, and this information will later be used to commit illicit activities.

- **Pharming** consists in attacking a website, making the most of its vulnerabilities in such a way that it makes it so that anyone who tries to enter it gets redirected to a fraudulent site which appears to be identical to the original site.

This attack makes the most of a vulnerability which is found the web pages' Domain Name Systems (DNS). The attacker achieves this by altering the translation process between the page's URL and its IP address. This way, when a certain domain name which has been subject to phishing gets entered, for example http://www.ciberderecho.com, the user will actually access the web page that the attacker has prepared to substitute it, which to an untrained eye probably looks exactly the same. The end goal is that the user introduces details (personal and bank) on this site that they are redirected to, and this data can be monitored, stored and stolen.

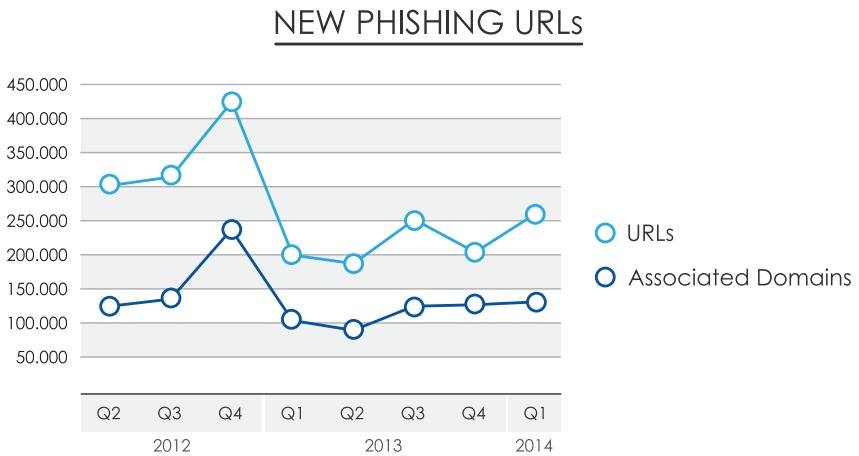
However, this technique can also be used via a modification in the HOSTS file which is found in the user's Windows system. This file allows the work of the DNS servers to be sped up, saving time for the internet service providers. When we write a URL in the search engine, the system checks if this address is found in the HOSTS file, and if so, the computer reads the IP address read the same and redirects to the web page. This way, if for some reason said file has been modified in the system by means of a virus or trojan, the attacker will direct the user to the web page indicated. To introduce the virus in the user's system, the attacker can use phishing techniques and, this way, by clicking on the URL in the email, the file with the malicious content is downloaded.



Screenshot of a phishing attack.
Source: Gmail email service

The difference between one and another consists in the means used to achieve the ultimate aim which is that the user introduces their details believing that they are accessing the web page that the wished to. Whilst with phishing, the deceit lies in the links which, just by clicking on them, direct users to other pages; with pharming, if an attempt is made to access the website, even by correctly writing the address (www.ciberderecho.com), the user is automatically directed to a fraudulent page which the attacker had ordered.

Both exclusively take place on online platforms due to the fact that they both exclusively involve cybernetic techniques. Because of the results that these techniques produce, in the territorial word they could be referred to as fraud, identity theft, or accessing information systems without the licensee's authorisation.



8.6.1.2 Analysis

For the territorial world, two fighting strategies can be found: either by the creation of a special law against cybernetic crimes; or, via a classification in the already existing Criminal Codes.

Examples of this first type can be found in Venezuela and the Dominican Republic which have special laws (Special law against computer-related crime of 30 October 2001; and Law Nº 53-07 on Crimes and Delinquencies of High Technology, respectively) which penalise the improper use of information technology to commit fraud, forgery of documents, the unlawful access to data etc. In this sense, both phishing and pharming are incorporated.

The Spanish Criminal Code is an example of the second type, whereby in sections 248 to 251 fraud is specifically understood as that which is committed via computer programmes and means.

The average sentence for these crimes in different territories sits at between 3 to 5 years of prison, together with varying degrees of economic fines.

The treatment of these conducts within the organisations that make up **cyber-world** differ:

- one the one hand, in terms of their classification, as they are not referred to as crimes, but prohibited or not permitted conducts;
- and on the other hand, in terms of the treatment of these conducts.

The most frequent answer to these conducts lies in the prohibiting of a range of techniques for identity theft, deceit, accessing websites to manipulate them, etc.

And so, we find that **Facebook** prohibits carrying out actions that could disable, overload or affect the correct functioning of appearance of their site. For example, the altering of the presentation of pages or another functionality, or the banning of gathering of the sign-in information of the accounts of other users. Furthermore, Facebook has a specific email which is available to users so they can report email messages which contain phishing:

What can I do about phishing?

Share article

Phishing is when someone tries getting into your Facebook account by sending you a suspicious message or link asking for your personal information.

Example: Joey gets an email saying he needs to log into his Facebook account and read an important message about his account. The email links to a strange looking website asking him to enter his username and password.

If you get a suspicious email or message claiming to be from Facebook, don't click any links or attachments. You can always visit **www.facebook.com** or open your Facebook app to check for important messages from us.

I think I've been phished. What can I do?

First of all, sorry to hear something might be wrong with your Facebook account. If you accidentally entered your username or password into a strange link, someone else might be able to log in. Here's what you can try:

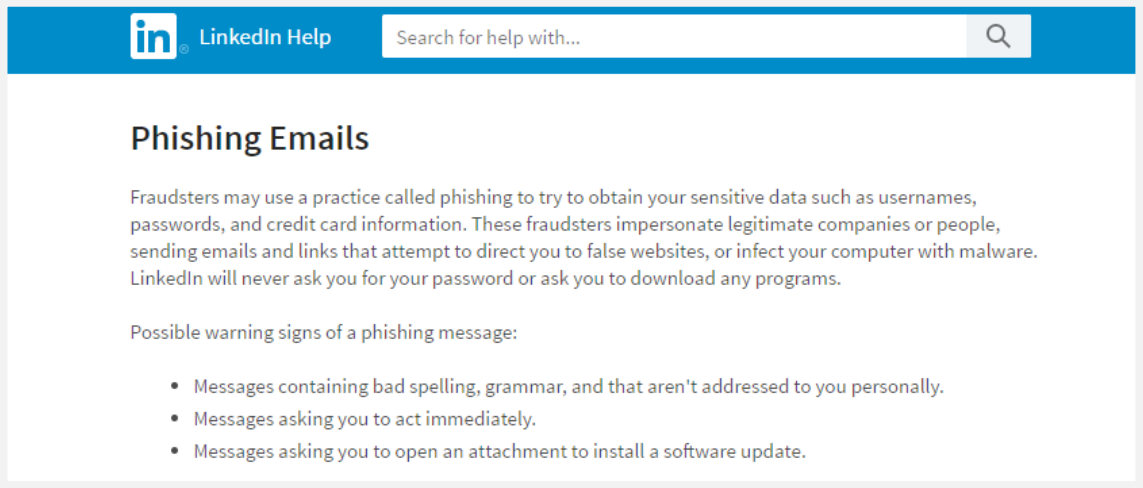
- Secure your account by resetting your password and logging out of any devices you don't own
- Recover your account if your username or password don't work
- Review recent activity to see if anything strange is happening to your account

If you get phished and someone else logs in, they may use your Facebook account to send spam. Learn More.

Facebook phising support. Source:
https://www.facebook.com/help/166863010078512?helpref=search&sr=1&query=phishing

Another example of this treatment in cyber-world can be found at **Yahoo!**. Here, impersonating other users, sending content which contains viruses, malware or malicious codes or has links to them, and collecting information and content about other users are all prohibited.

Linkedin meticulously deals with each possibility of these conducts, and it prohibits, for example, the manipulation of identifiers to hide the origin of messages or publications through their services, and the creation or operating of pyramid schemes, frauds and the like. Although the treatment of these conducts do not differentiate the techniques by which they are carried out, there is a specific section for the solving of these problems and there is an email address available in order to report emails which could be considered as phishing.



LinkedIn's support for phising attacks. Source: https://www.linkedin.com/help/linkedin/answer/9492?lang=en

8.6.1.3 Proposed solutions

The elaboration of the recommendations and measures which are necessary to combat the phenomenon of phishing and pharming must be centred in the cyber-world which, in the majority of current cases, is home to bank fraud.

The only exactitude that is possible is with respect to **a state-wide level and to organisations** and it consists in the task of coordinating with the authorities and citizens to warn about and report frauds that are carried out in relation to their brand and their products. When faced with a series of known phishing and pharming attacks, it is fundamental that

- Organisations warn about their existence and the correct measures to avoid them.
- Client care services are available to solve all queries.

On a **personal level**, should there be any sign of suffering from an attack or of being attacked via phishing/pharming techniques, the following actions should be adopted:

1. Do not enter any personal data, passwords or user names in sites that are not verified as secure sites (a HTTPS address, a locked or green padlock or any type of certificate which verifies secure web surfing)

2. Immediately stop surfing the web if anything suspicious is detected, close all widows and tabs.
3. If details have been entered, in each case contact:
    - Banking entities.
    - Phone companies.
    - Card companies to block any unwanted transactions.
    - Local authorities, if it the object of fraud is detected.

The aim of this contact is to secure the data and to ascertain that transactions will not be made by third parties without the card-holder's authorisation.

4. In any case, change passwords, verify the correct access to all accounts and verify the integrity of the data.
5. If there is an antivirus available, run a scan of the device and a cleaning of the possible malware or virus that could have been installed.
6. After having left a record of such, deleted all the messages which contained the fraudulent links, reporting them as phishing or spam.
7. Later, and in addition to the above, the organisation or entity whose web site was under attack should be contacted and warned about the problem, by means of a safe, verified way.

9 Cyber-police

The revolution of the internet and its change of paradigm have created new social conflicts in a new world called cyber-space.

In this new, virtual, global world with no borders, the efficiency and legitimacy of legal powers is limited, which has led to legislators making new attempts at passing regulations that try to create legal order, thus making their power prevail.

A clear example of these attempts is the recent amendment to the Spanish Criminal Code, which in sections 282 and 588 d, e and f, creates the figure of the cyber-police. Who is this figure and what are its aims?

With the passing of this reform, cyber-police become civil servants which, authorised by the territorial regulations with the power of the Law, perform cyber-security controls on the internet, such as for example, pro-active surveillance, or reactive and defensive actions in order to maintain civil order, avoid cyber-conflicts and mitigate risks. In summary, they try to achieve a greater security within cyber-space.

Therefore, with this there is a clear aim: controls in internet security.

Moreover, and controversially, the police will start to use technological tools for the cybernetic defence-attack. This way, cyber-weapons will be born.

In this regard it should be remembered that a conventional weapon can be defined as a tool which amplifies the strength to cause damage, or as an instrument, means or machine designed to attack or defend.

Following this definition, the cyber-weapons can be defined as "the cyber-applications used to attack and cause cybernetic damage" or as cyber-tools for defence. In this regard, the Spanish Criminal Code highlights the following:

"Section 588 f. a. 1. The competent judge will authorise the using of identifying data and codes, as well as the installing of software which permits, in a remote and electronic way, the examining the computer, electronic device, information system, massive data storage instrument or database from a distance and without the owner or user's knowledge, providing that this is in the interest of an investigation of one of the following crimes:

***a)** Crimes that are committed within criminal organisations.*
***b)** Crimes of terrorism.*
***c)** Crimes committed against minors or persons with a legally reduced capacity.*
***d)** Crimes against the Constitution, of treason and regarding national defence.*
***e)** Crimes committed via information instruments of any other information technology or telecommunication communication service.*

And as security should be understood as the lack of risk, and risk as the possibility of harm occurring, what is truly important is the use of these weapons, rather than the weapons themselves. For that reason it is said that security is not a product, but a process, where what is important is the application of control services which help to mitigate future risks. And that is precisely what the cyber-police do, they provide control and surveillance services for public security.

From there, the Spanish Criminal Code claims to follow the same simile and it legitimises the use of cyber-weapons in the hands of cyber-police that carry out cyber-surveillance on the internet, to then assure and avoid possible harm to the cyber-citizens.

However, this causes necessary diverse and important legal questions of great social significance- in what field and who are they protecting? Who controls the cyber-police? What empowerment and legal regulations is the Spanish Criminal Code trying to achieve with this?

As far as I am aware, all of these will require a large study, dissemination and implication of the different actors. Amongst those, the executive and legal branches, lawyers, sociologists and economists that are specialised in new technologies should be implicated in order to deepen and discuss how praiseworthy legislative aim can affect other fundamental rights and freedoms.
Or however, so that continental law does not fall behind the technological revolution, these "social agents" should start to study new legal, intangible and global assets, to order in cyber-space, such as cyber-freedom and cyber-privacy.

Legal arguments in favour of the cyber-police:

1) For reasons of National Security and Cyber-security, the State should be able to carry out public surveillance functions in order to avoid security problems instead of leaving control of these elements in private hands.

2) Cyber-space raises challenges for the State Agents and Security Forces that are overwhelmed with the current tools and they need a clear, enabling legislative framework in order to prosecute cyber-crimes in the most efficient way.

Legal arguments against the cyber-police:
1)This cyber-figure and the cyber-surveillance activities that they carry out affect the individual liberties of people who surf through cyber-space, widely surpassing their supposed role of a guarantor of cyber-security.

2) This cyber-figure does not advocate for cyber-freedom or freedom in a new virtual environment. From this point of view, the State is presented as a threat and like a "Cyber Big Brother" which does not see any limits to its power.

My legal point of view
Freedom ends when it affects the freedom of another. With the arrival of the internet, new problems have arisen that call this principal into question.

Cyber-crime is a current reality, and cyber-criminals make the most of this legal vacuum (lack of legal and legislative power) in cyber-space in order to commit their acts, but the solution lies in proportionality and moderate relations

It is not necessary to advocate for the lack of regulation and the leaving of cyber-space to order itself based on self-regulation, as that would involve cyber-citizens defending their rights in a private and individual way, not for the collective good. Likewise, it is not necessary to give so much power to the State, as without specific control mechanisms, a great amount of this surveillance data can be used against the public interest of the citizens.

The moderation and proportionality lies in the creation of the figure of the cyber-police. Meaning, creating regulated bodies with strong legal guarantees, such as for example the investigation by information means only if there is a sign of criminal activity and with this should be in proportion to the crime that is being investigated.
However, the role of the regulation, whilst still being adequate to solve the problem, continues to be limited to the State's legal orders and the borders established by our country.

In conclusion, the proposal of the Spanish Criminal Code is limited as it is local and territorial. In other words, it tries to solve a cyber-problem or cyber-crime, which is global, with territorial measures. For example, a cyber-policeman will not be able to defend or go after a cyber-behaviour which was carried out by an individual in a different State with a different jurisdiction.

10 Antisocial cyber-behaviour against the right to privacy, honour and image rights.

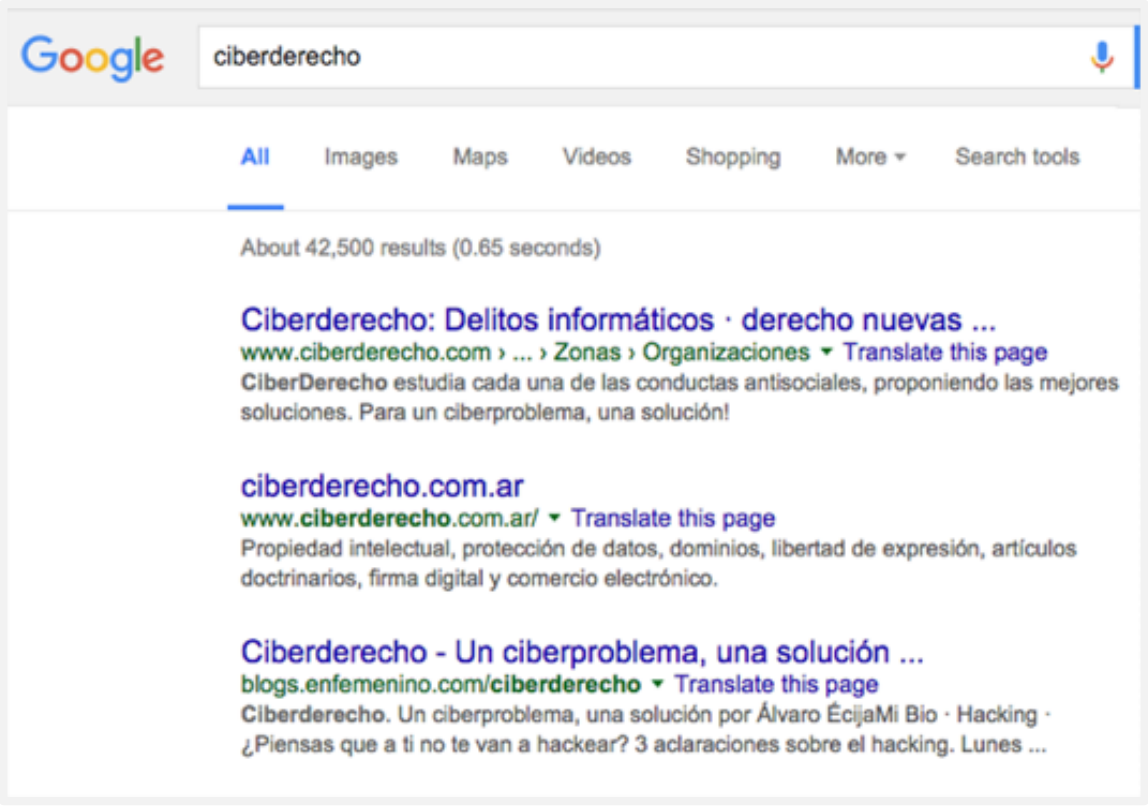
10.1 Treatment of data in search engines. The right to be forgotten

Since 2014, first in Europe, and gradually throughout the rest of the world, a new right as been legally recognised regarding the cybernetic world whose repercussions have not stopped growing and it is predicted that it will get to the stage where it is so relevant that it conditions the future of organisations and their regulations in coming years. This is in regards to the so-called right to be forgotten, which is linked to the treatment of personal data being found on internet search engines (Google, Bing, Yahoo!) without consent.

10.1.1.1 Scenario

The treatment of this data by internet search engines happens when carrying out a search on Google or Bing, the search brings back results which contain personal data.

For example, when carrying out a search of the term "ciberderecho" (cyber-law in Spanish), the third result that Google comes up with contains personal data.



Example of a Google search.
Source: google.com

In reality, the information is not originated on the search engine (as can been seen in the image, it is www.ecixgroup.com which generates it); but what they do is gather the information that is on that web page as display it as a result (this action is known as indexing).

However, the fact that the search engine has not created this information does not mean that it is not dealing with personal data and that, therefore, they are not responsible for said treatment. For this reason, at a European level, the search engines that operate in Europe operate under data protection regulations.

The workings of this are simple: the information is found on the internet, and the search engines facilitate access to such. In normal circumstances, this information of any sort, does not have to be harmful towards the interested party. However, the problem occurs when the information displayed by the search engines is harmful, be that either on either a personal or professional level.

When dealing with this treatment of data, the so-called **right to be forgotten** can be applied. This is that faculty that citizens and interested parties have to request that search engines remove search results that contain personal information (i.e. a CV or a photo).

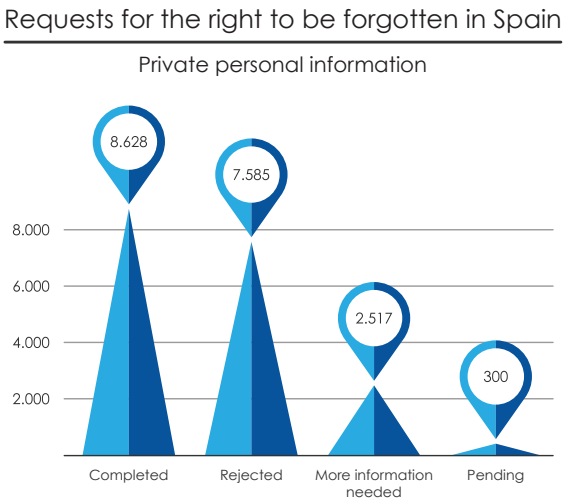
- It is not right per se, although it is popularly known as such, it is an action which can been carried out thanks to other rights, such as the right to the respect of private and family life and the right to the protection of personal data (Articles. 7 and 8 of the EU Charter of Fundamental Rights). However, this is popularly summarised as the right to be forgotten.

- Although any request for the removal of information from the internet is popularly referred to as the right to be forgotten, in reality "the right to be forgotten" is legally the request that is made to internet search engines. To request the removal of personal data from a specific web page, the channel of exercising the right to the cancellation and/opposition to the data protection regulation can be used.

- One of the points of balance of the right to be forgotten is that the information can continue to be published on the original web page and therefore the freedom of information/speech is still in force. However, it mitigates the prejudice that said information caused to the citizen as although that information continues to be published, it cannot be found easily by typing their name and surname into the search engine.

- It is a jurisprudentially created right and it is not complete as there are some application conditions and limits.

The impulse to the right to be forgotten arises as a result of a preliminary ruling brought to the European Court of Justice by a Spanish court due to a Spanish citizen's request to Google and a local newspaper to withdraw certain damaging information from the internet which was obsolete. In May 2014 the Court of Justice ruled in favour of the citizen regarding the search engine, and from that moment the right to be forgotten has been demanded by interested users.



[5]

10.1.1.2 Analysis

The treatment or indexing of personal information and data by search engines involves the handling of personal data and due to this, they consider themselves responsible for the handling of that data on their services.
According to the European Court of Justice (ECJ from henceforth) this condition is a determining element so that citizens can request this right, if the treatment is not considered to be correct, improper or excessive.

Independently of the position that the web page that houses the information takes regarding a request for the removal of said personal information; search engines must proceed to eliminate the required personal information from their search results if they meet the requirements established by jurisprudence.

As has just been indicated, the request for the exercise of this right must be valued case by case, and not one case can be an absolute right.

- First of all, a consideration must be made of the conflicting rights, in terms of the circumstances of each piece of information and each request. For example, if the information regards someone's professional activities, the informative interest of said information must be studied, if it contains sensitive information (such as their religion or sexual orientation) which could be harmful to the individual, or if on the other hand it is journalistic information, etc.

- Second of all, the exceptions that the ECJ establish for not applying this right must be taken into account:
    - Information which is relevant to the public or makes reference to a public person which sparks informative interest.
    - Exact information.

[5] Requests for the Right to be Forgotten in Spain up to 2015. Source: Google.

- Information that is not obsolete.

It does not include the results gained through any type of search; instead it only involves the searches performed by introducing the name of an individual, as that search may lead to the obtaining, by means of a list of results, of a structured vision of information regarding that person that can be found on the internet and it allows for the establishing of a quite detailed profile of said individual.
Furthermore it is necessary to draw attention to the fact that the original information **will still be accessible by using other terms, or via the direct access to the website that published the** information.

Finally, in terms of territorial application, this can first of all be defined as a right which is only applicable in Europe, however it has been configured to the extent that it has been consolidating as a right which is applied further beyond Europe, expanding it to the dot com domains and to all those that are accessible from Member States.

Currently, we can only find its application in the diverse European countries, with Spain leading the pack, and only a tenuous application in Argentina and Mexico, where, mirroring the ECJ's ruling, the national courts have established the need to offer their citizen's the change to exercise this right should they so wish.

In terms of the importance of the right in question, in figures some 78% of those surveyed consider that service providers have too much information about consumer's behaviour and preferences[6]. More than 6 in every 10 Europeans (63%) say that the disclosure of personal information is a large problem for them. And only 22% of European citizens completely trust internet companies such as search engines, social media and email services.[7]

10.1.1.3 Proposed solutions

The exercising of the right to be forgotten that is currently being applied is one of the most correct ways of dealing with the unwanted handling of data on search engines.

State and organisations must have channels of communication available to citizens through which they can manage their right to be forgotten:

The organisation, the search engine in this case, should have a visible link available through which a form can be easily accessed to make this request. Additionally, if a quick information guide was made available about the right and the process, citizens would be more informed.

It is recommendable to remind the citizen that, complementary to the exercising of the right to be forgotten, if they wish for certain data to be withdrawn or deleted from the web, it is necessary to approach the pages that host this information to request its removal as that is the most efficient way to avoid it being indexed by search engines.

[6] Loudhouse survey, 2014
[7] Eurobarometer, 2011

Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea

Antecedentes

Un fallo reciente del Tribunal de Justicia de la Unión Europea (C-131/12, 13 de mayo de 2014) permite que determinados usuarios soliciten que los motores de búsqueda eliminen resultados de consultas que incluyan su nombre si los derechos de privacidad de la persona prevalecen sobre los intereses en esos resultados.

Al realizar esa solicitud, Google realizará una ponderación entre los derechos de privacidad de los usuarios y el derecho del público a conocer y distribuir información. Al evaluar su solicitud, Google examinará si los resultados incluyen información obsoleta sobre usted, así como si existe interés público por esa información (por ejemplo, Google puede negarse a retirar determinada información sobre estafas financieras, negligencia profesional, condenas penales o comportamiento público de funcionarios del gobierno).

Para completar este formulario, necesitará una copia digital de un documento de identificación. Si envía esta solicitud en nombre de otra persona, tendrá que proporcionar un documento de identificación de esa persona. Los campos marcados con un asterisco * se deben completar para poder enviar su solicitud.

Seleccione el país cuya legislación se aplica a su solicitud. *

Seleccionar uno

Información personal

Request to Goggle to take down content.
Source: google.com

If approaching the organisation itself has not led to the results that the citizen wanted, States should have a secondary channel of communication available to watch over the right to be forgotten.

In this regard, Spain has a control body available, the Spanish Agency for Data Protection, which can be turned to should a search engine not resolve the request to exercise the right to be forgotten in a satisfactory way. This assures the correct protection of the right to be forgotten for that citizen which requests so.

However, as far as I understand, it would be recommendable to have a Cyber-Court or Cyber-referee that could resolve when the requirements mentioned in the aforementioned ruling are fulfilled and when they are not. Furthermore, this Cyber-Court should put an agreement together for the search engines and institutions in the European Union.

The citizen must be the person who is interested in the deletion of the internet links which contain the personal information in question. The necessary information should be made available to them regarding the mechanisms which exist to exercise their right. Specifically, they should be able to have the following options:

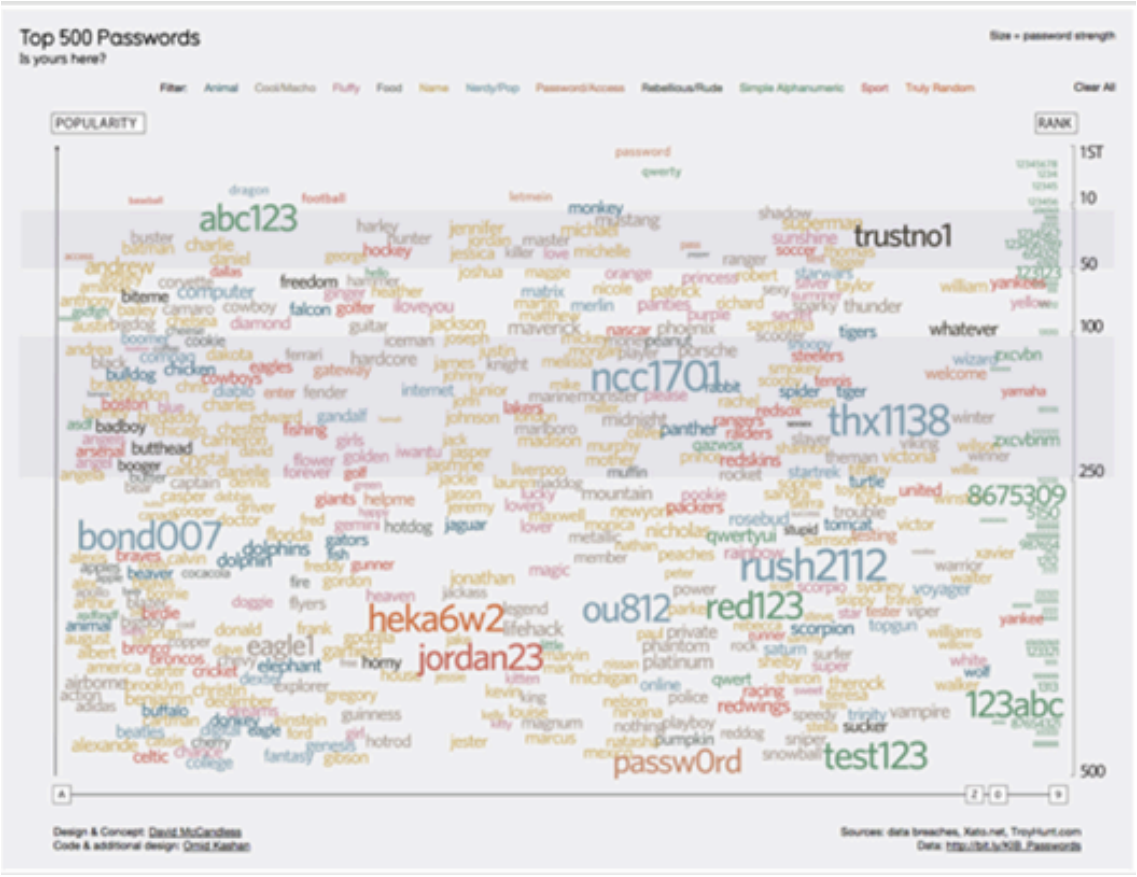
1st- turn to the search engines to be able to request the removal of information concerning their person.

2nd- turn to the appropriate state/supranational control body to defend their right; they should also be given the necessary help to complete the request in a satisfactory fashion in order for the search engines to remove search results regarding their person if they had not done so beforehand.

10.2 Access to content without authorisation

Of all the conducts of easily accessing a medium level user, the accessing of contents without authorisation is the most frequent. If the victim just pays not enough attention for

a second and their log-in details for any account are known, actions that make up part of this conduct can be carried out.



500 most common passwords on the internet.
Source: informationisbeautiful.net

10.2.1.1 Scenario

The access to content without authorisation involves accessing of information and data of third parties, be that personal or private, which is done so by means of any sort of illicit or non-authorised method.

On the internet, accessing content can be realised by methods such as identity theft, spyware, phishing or the infection of computers by information viruses, which gain access to the information or computer or technological media. The data which is most frequently object of this is always of a personal or private nature.

Just as with espionage, the information technologies encompass a new field which introduces tools, some are still to be created, for the tracking and collecting of information and a space in which to store all types of data.

In this case, the data which is most frequently object of this is of a personal, private or confidential nature, such as bank details or economic data of phone or internet accounts, etc., or even data regarding personal and affective relationships.

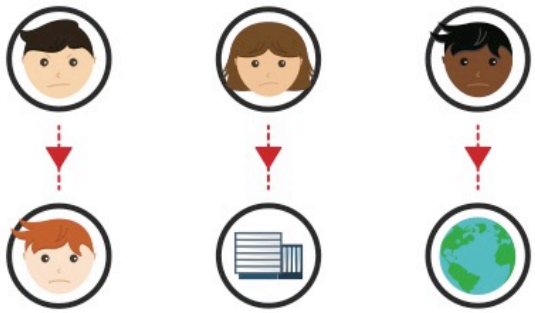
There should also be an assessment of the devices which can give way to this behaviour, as on this occasion they are not limited to personal computers; cyber-espionage can take

place on any technological device: tablets, smart phones, storage devices, etc. Every system and device with the capacity for the entering and leaving of data is susceptible to being a target for this type of behaviour.

How this Happens

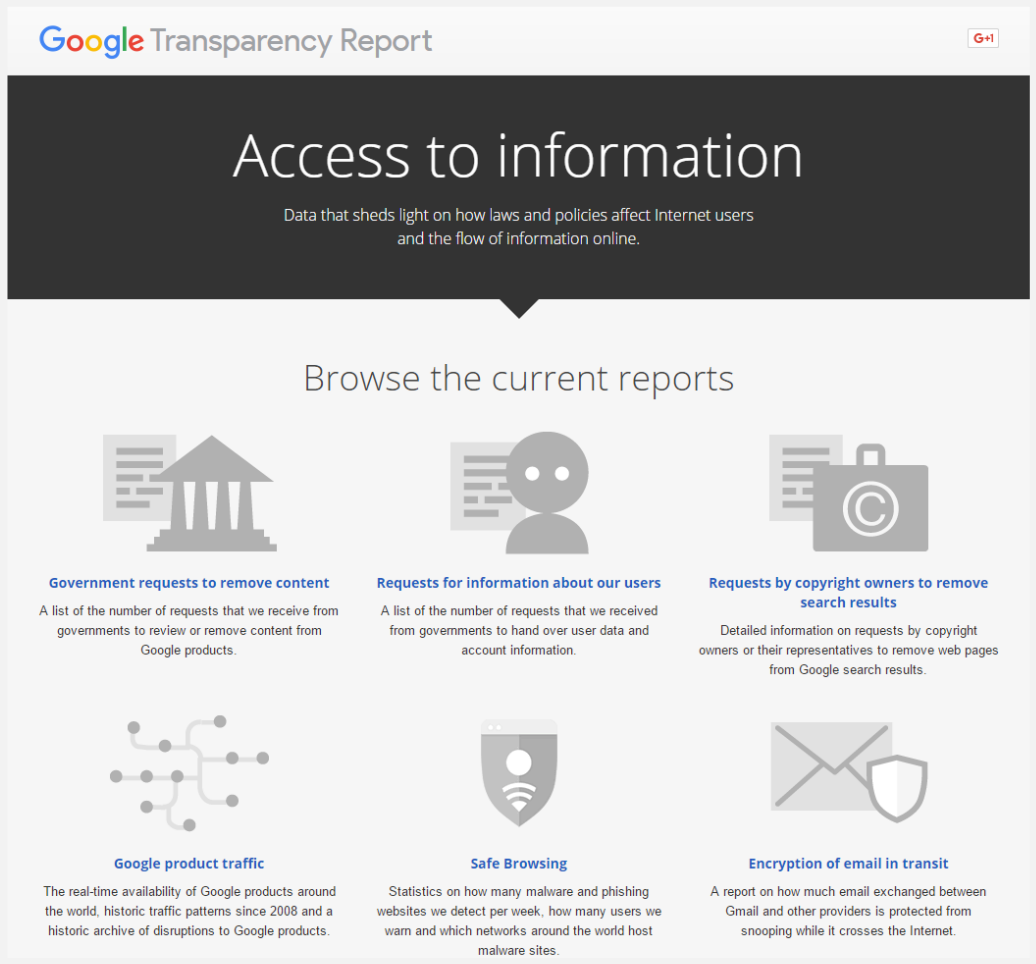
- **Individual-Individual:** A cyber-user obtains information and personal data, via their personal computer, smart phone or tablet.
- **Organisation-Individual:** A cyber-user is spied on by an organisation, which gathers data and information about him/her.
- **State-Individual:** A State gets an individual's information and personal data, once again this can be via their personal computer, smart phone or tablet, as well as through the different official registers and mechanisms.

In this regard, it is becoming normal for States to request information to Organizations about their users. In this sense, it is the organisation that we have a relationship with that can give over the information about the requested user and this can be extremely diverse: from income registers to phone records.



Some organisations, such as Google, have a portal called the transparency report which is available to users[8], with the requests that have been asked of them:

[8] https://www.google.com/transparencyreport



Google's transparency portal. Source: https://www.google.com/transparencyreport/?hl=en-GB

10.2.1.2 Analysis

In the territorial world, the illicit or non-authorised access to content tends to be dealt with in the Criminal Codes that can incorporate a section on behaviour in the computing environment, or even through special criminal laws.

An example of the first case is that of **Bolivia**, whose Criminal Code establishes in article 363 ter the crime of altering, accessing and wrongful use of computer data.

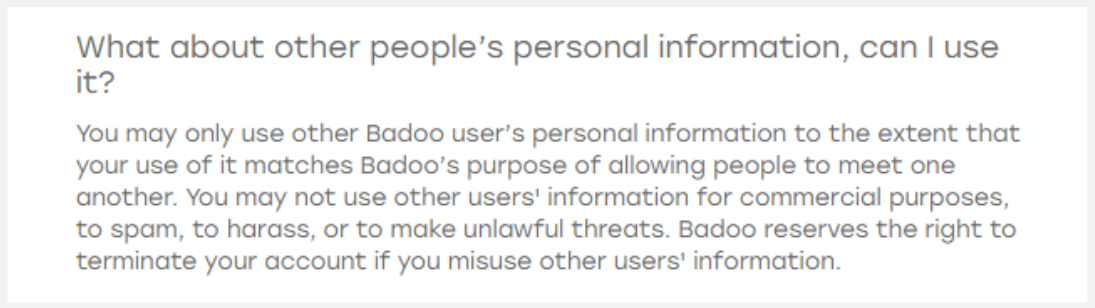
On the other hand, **Peru** is an example of the second case, which deals with and penalises this type of behaviour in Law 30.069 on Computer Related Crimes. The action of accessing all or part of an IT system without authorisation is considered a crime, providing that this was done by violating security measures that were put in place to stop such actions. For these cases, perpetrators are sentenced to terms of imprisonment.

In cyber-space, the access to content without the owner's permission is expressly prohibited in the Terms and Conditions of each organisation, with it being a frequently mentioned behaviour in the self-regulating texts that they all have.

On **Aliexpress** the Terms and Conditions establish the following in terms of behaviour regarding the unauthorised accessing of content :

- Users cannot copy or display services or any information, text, image, graphic, video, sound, directory, file, database or list etc. that is available through Aliexpress.
- They cannot collect content from the site to create lists, databases or directories.
- Likewise they cannot make use of any content for any aim that is not expressly permitted within the Terms and Conditions.

The unauthorised access to content on **Badoo** is a behaviour which is limited in the Terms and Conditions, establishing for example:



What about other people's personal information, can I use it?

You may only use other Badoo user's personal information to the extent that your use of it matches Badoo's purpose of allowing people to meet one another. You may not use other users' information for commercial purposes, to spam, to harass, or to make unlawful threats. Badoo reserves the right to terminate your account if you misuse other users' information.

Information about Badoo's Terms and Conditions. Source: https://badoo.com/en/terms

11 Virtual Money

11.1 Bitcoins

Through the popularisation of games online and on social media, the bitcoin offers what appears to be an alternative payment solution which is better adapted to the particular needs of the exchanging of virtual goods or services. These measures have confirmed it as an alternative which aims to play the same role in cyber-space as cash does in the real world.

Despite its proliferation, the market's attention is concentrated on just a few initiatives which have proved successful on a global level, amongst which bitcoins stand out due to the presence in the media.

11.1.1.1 Scenario

Among equals or P2P, the bitcoin can be described as a cyrpto-coin. In other words, it is a digital currency used to perform relatively secure anonymous transactions without the need for a centralised authority. Instead of being emitted by a banking system, it is Bitcoin users themselves who create the currency by using an open code software and an intelligent algorithm which facilitates the security and anonymity of the entire system.

Bitcoin is based on a decentralised operative model. This means that there is no authority which takes responsibility for its emission or for the recording of the movements that it produces. In its place, it is supported by a Person-to-Person distribution network, via connections between the users of this currency (this resembles the decentralised exchange of digital archives such as music or films, via Bitorrent).

From the user's perspective, Bitcoin is nothing more than a mobile or desktop application which provides personal Bitcoin coins and allows them to be sent and received by users.

From a development and programming perspective, Bitcoin shares a public accounting called "block chain" which contains each processed transaction, allowing for the validity of each one to be checked. The authenticity of each transaction is protected by digital signatures which correspond to the mailing addresses, allowing users to have total control over the sending of Bitcoins.

The cyber-behaviour which can be produced with Bitcoins includes everything related to the monetary world and with commercial and monetary transactions. And so, Bitcoins can be used as an instrument for money laundering, drug trafficking, bank fraud, online games or any other similar operation.

The Bitcoin has become the most famous virtual coin to date.
Source: depositphotos

All of these conducts are exclusively produced on the internet, as Bitcoin is a purely virtual currency with no trace in the physical world (in fact, its representation is nothing more than the renderings of the symbol of the Bitcoin, as there are no factories which make coins or print notes with these characteristics).

It is precisely the operating of this currency which fosters the appearance of these previously mentioned conducts. As there is no need for a central authority which manages the Bitcoin, as the system controls itself and is anonymous and without supervision, it can be very useful for drug traffickers, sellers of weapons, or any other business on the black market.

Although in the same regard, the fact that there are mechanisms which are independent from the system, through which the anonymity of the network can be notably reduced, together with it being a transparent system, may prove a great threat to the privacy of its users.

Likewise, with this being a system which is entirely based on a computer system (without a physical currency), its implementation is liable to possible programming errors and weaknesses that can be exploited by malicious users to access the balance of users, although it does have an advantage compared to physical currencies in that **it is not inflationary. Unlike a fiduciary currency, which can be printed to create more, the Bitcoin is designed to have a maximum number of units. In total, a maximum of 21 million units can be created, following a predetermined algorithm.**

Furthermore, the nature of Bitcoin makes the system totally dependent on energy consumption, which is necessary to make the complex calculations which are required for it to work, thus participating in a network involves a cost for users who in the long run will not be compensated with the benefits obtained.

One last problem regarding the operations carried out with Bitcoins is the speculation that they are seen to be subject to a market which works in favour of the speculators. As it is

not supported by any kind of Central Bank or governmental or international organisations, the Bitcoin suffers from periodic fluctuations depending on the interest of the speculators that make transactions with it, which is another element to add to the risks that can be suffered from when operating with this currency.

History of the number of Bitcoin operations.
Source: Blockchain.info

History of the value of Bitcoin operations.
Source: Blockchain.info

Summarised what has been analysed, the Bitcoin can be broken down into the following characteristics:

a) It does not belong to any State of country and it can be used world over.
b) It is decentralised: it is not controlled by any State, bank, financial institution or company.
c) It is impossible to forge or duplicate thanks to a sophisticated cryptographic system.
d) There are no intermediaries: Transactions are made directly from person to person.
e) Transactions are irreversible.
f) Bitcoins can be exchanged for euros or other currencies and vice versa just like any other currency.
g) Identity does not have to be revealed in order to do business, and thus privacy can be kept.
h) 100% of the money belongs to the user; it cannot be intervened by anybody and accounts cannot be frozen.

11.1.1.2 Analysis

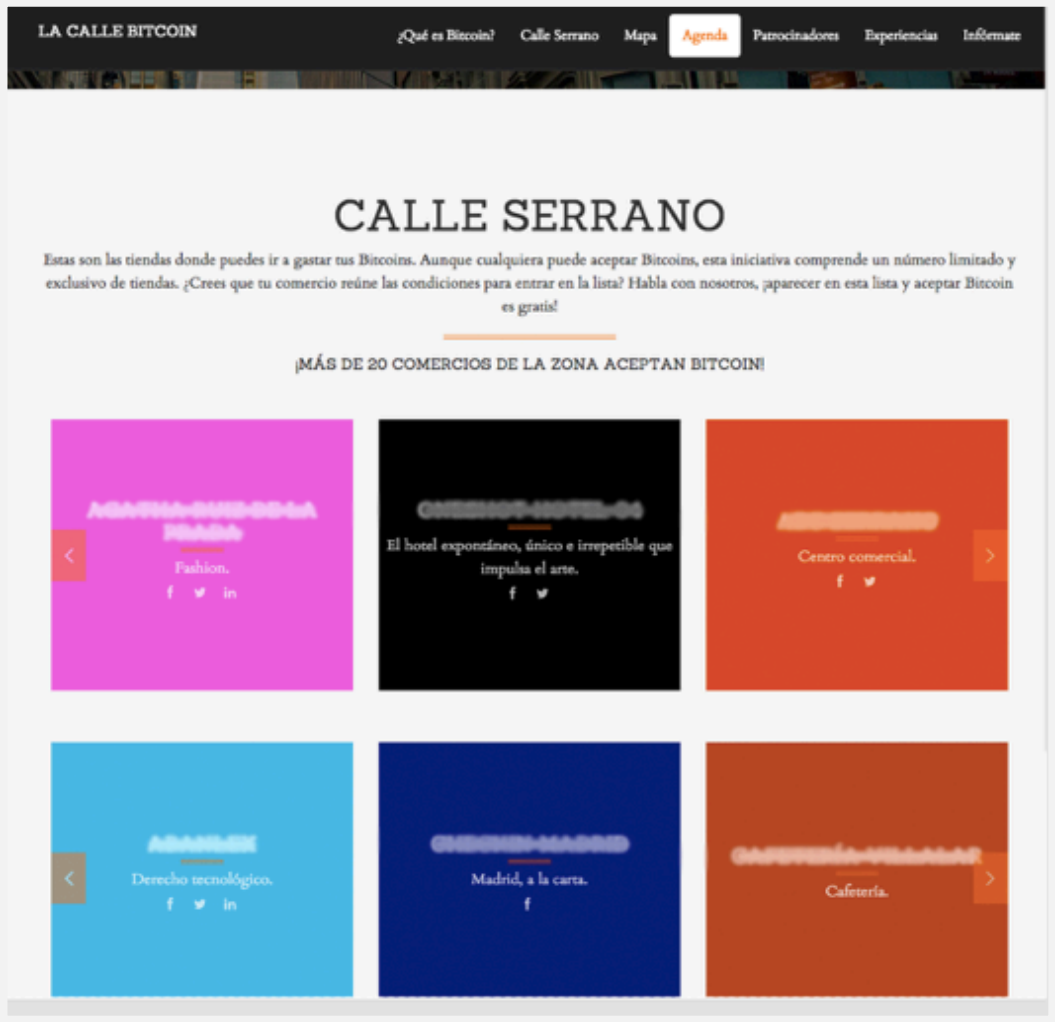
The differences in the conducts regarding the Bitcoin compared to other conducts lie in terms of its regulation. As it stands, not one State in Latin America or Spain has a Law, Directive or Regulation dedicated to regulating the use of Bitcoins.

In the territorial world the unregulated nature of the Bitcoin prevails as nowhere has come out either in favour or against its existence. The majority of Central Banks in different territories have expressed that it is not a valid currency which is supported by their systems, however this has not been expressed in regards to other legal status that can be held. The idea is currently being consolidated of treating the Bitcoin as a thing, as an object.

The journey towards legality and effectiveness right now has to go through some **legal voids** where transactions can be carried out with normality, as is the case with **Spain**, where the defenders of this virtual system classify it as an exchange, which is allowed in their legal systems, entailing of a system where assets are exchanged for other assets by the will of the parties.

In terms of the cyber-behaviours carried out with Bitcoins which have an impact in the physical world, these have not been mentioned in the regulations of the different territories either. Therefore, the generic rules would have to be turned to and each case would have to be studied on an individual basis to see which rules would apply.

As an additional fact, initiatives are starting to emerge to incorporate the Bitcoin into the physical world, such as the Spanish initiative "La calle Bitcoin" (Bitcoin Street) whereby twenty odd business in one of the most commercial areas of Madrid have joined together to accept payment via this method.

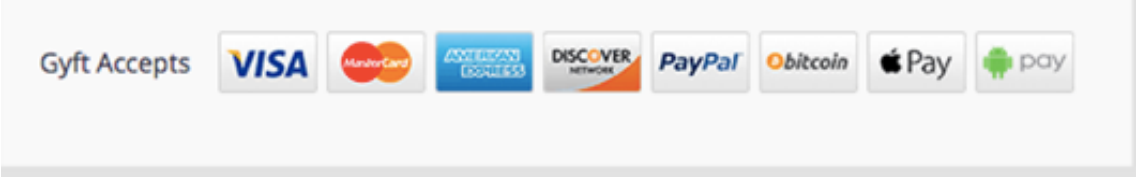


Example of physical businesses that accept Bitcoin payments.
Source: http://callebitcoin.es/spanish.html

In the cyber world this situation is split between those organisations that allow Bitcoins to be used as a means of payment, and those which only allow official currencies. The majority currently fall into the second category.

Due to the fact that there is not a single regulation for a sector of internet organisations, or for a group of them, each organisation is free to accept the payment methods that they so wish.

Portals such as **Destinia**, **Wikipedia**, **Wordpress** and **Reddit** and organisations such as **Dell** already admit payment in this format, but there are lots of organisations that have not taken this leap of faith.



Example of physical businesses that accept Bitcoin payments.
Source: callebitcoin.es/spanish.html

The rules in this regard are regulated in the Terms and Conditions of the organisation which admits said payment, allowing the system to have complete freedom over the management of these payments.

11.1.1.3 Proposed solutions

The proposal for a solution to deal with the Bitcoin situation needs to take the form of a common agreement between a group of influential internet organisations in order to adopt the regulations proposed regards the parameters of the Bitcoin.

The role that the organisations play is fundamental if they do not want to lose the opportunity to influence the payment methods that will reign over the internet in the future.

Out of all of the possible measures that could be adopted, these three stand head and shoulders above the rest:

- Creation of a normative framework of the conduct.
- Cooperation between organisations, evaluating the possibilities of creating a global legal framework.
- Encouraging the expansion of the Bitcoin as a payment method.

Likewise, as a reflection in the physical world, the biggest obligation that arises is in terms of the States, which should take the following measures:

- Creation of a regulatory framework of the conduct:
- Establish channels of dialogue with the cyber-organisations in order to manage the transactions.

12 Intellectual Property on the Internet

12.1 Cyber-piracy

In the world of intellectual property, the most frequent cyber-behaviour that is found online is the cyber-piracy of a whole range of content. This is a phenomenon which increases year on year, becoming more important as time goes on, and it has serious consequences for the economies of different States.

12.1.1.1 Scenario

Piracy or **copyright infringement** is made up of the illegal appropriation, copying and distributing of work which is protected by copyright or is someone else's intellectual property, for example films, books, music, video games, software, or anything else which, through the different methods available, can become available to the public.

This is different to **forgery,** which also violates industrial property rights, in that the latter involves distinct objects and matter such as merchandise and packaging or industrial designs.

On the internet, **cyber-piracy** has the same definition, however its only means for appropriation, copying and distributing the material obtained is via cyber-space, as cyber-piracy takes place on the web and needs it in order to exist.

- **Perpetrators:** are those who appropriate, copy or access content in order to make it available to the public, and also those that allow and facility making the content available.
- **How this happens:** The most common way of committing cyber-piracy over the internet is by using P2P file exchange networks and Torrent file formats.
- **Types of work:** All types of work are susceptible of being transmitted or stored in the digital world. Live sporting events (such as football) and foreign TV series and films (mainly from Hollywood) and those which are especially susceptible to this type of conduct.

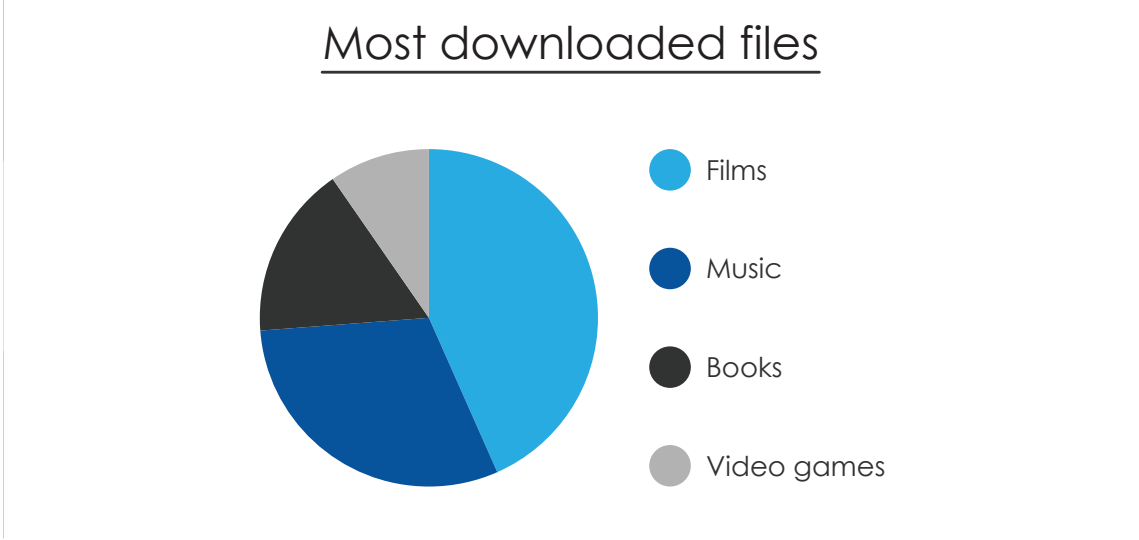
RojaDirecta, the web streaming site of sporting events that has been most accused of piracy in Spain. Source: rojadirecta.me

Cyber-piracy leads to conflict between the authors and companies which hold the different rights and the citizens and internet users, and it provokes debate regarding which motives should be prosecuted to a greater or lesser degree and the seriousness that should be placed on this type of action.

In figures, cyber-piracy is deep-rooted within society. For example, in Spain some 51% of internet users admit to having illegal accessed content: most commonly, 43% have accessed pirate films, next in line is music with 28%, books with 15%, and some 10% of the population have illegally accessed video games online[9]. The remaining Spanish speaking countries are not far behind. It is estimated that around 59% of the software used

[9] GfK April 2014 | Observatorio de Piratería y Hábitos de consumo de Contenidos Digitales 2013

in digital media in Latin America comes from pirate sources. [10]



12.1.1.2 Analysis

Unlike the other cyber-behaviours, whose incidence rate or appearance has arisen fairly recently, violating copyright or intellectual property rights has been more common, although by means other than the internet. For that reason, the different States and organisations have well established protections against this type of behaviour.

In the **territorial world** it is common to find specific laws regarding intellectual property and copyright, and provisions regarding the corresponding sentences are found in the different Criminal Codes worldwide.

To give an example, throughout the **USA**, copyright violations is penalised with prison sentences of between 5 to 10 years, depending on the seriousness of the conduct and the harm caused, and this can be complimented by economic sanctions too. (As stated in articles 2319 et seq. of the U.S Copyright Act).

France, on the other hand, imposes lesser sentences. Section L335-4 of the code on Intellectual Property penalises acts of reproduction, public communication or spreading of protected work and other conducts related to these actions with sentences of 3 years imprisonment and fines of up to 300,000 euros.

These conducts are not specifically referred to as cyber-piracy, but instead they are included underneath the umbrella of general violations to rights, or they are added in a sub-section dedicated to the committing of these crimes by using technology.

In the **cyber-world**, all organisations structure their terms and conditions with a section which is especially dedicated to intellectual property and the violation of these rights. Moreover, in the section about prohibited behaviour or prohibited content, they always establish that violating these rights is not permitted. This is especially true in the case of information or content trading organisations.

[10] BSA Global Software Survey, June 2014

For example, **Vibbo** specifically mentions the prohibition of "spreading, transmitting or making available to third parties any type of information, element or content that involves a violation of intellectual or industrial property rights, patents, brands or copyrights that correspond to the licensees of the portal (in reference to Vibbo) or to third parties."

In its content Policy, **Amazon** outlines a whole range of specific prohibitions regarding copying, translated or dubbed versions, recordings and unauthorised reproductions of books, music, films, videos, software, images and data copied from one format to another, etc.

Additionally, in the section on the Terms and Conditions, both organisations detail the previously mentioned conditions, making communication channels available to users which are specifically directed towards the protection of these rights (in the format of a form). This is of utmost importance as none of the organisations have specific sections and forms for other cyber-crimes which are equally important.

DAILY NEWS 29/10/2015

The most popular streaming page (for films and series) after the disappearance of **#Megaupload** and **#Seriesly**, has closed after various months of conflicts with the authorities in different European countries, Spain being one of them.
The well-known film and series streaming website and application became a leader in the sector of this type of web pages thanks to the 720p and 1010p HD torrents that it achieved through other external torrent services, and by widening then range of films and series that it had available, which users could access without having to register.

This site, just like its predecessors, was in the sights of the key cinematography producers and distribution companies which accused it of repeated crimes against intellectual property.
Beyond the permanence of Popcorntime through other cloned pages, or the possible sanctions that are able to be imposed on those responsible for this initiative, it is important to know the reasons why these types of pages are accused of **#piracy** or **#cyberpiracy** **and the reason for which those responsible have decided to stop this activity.**

12.2 Cyber Trade-Mark Abuse

The second most common cyber-behaviour on the web in terms of intellectual property is third party trade-mark abuse. The internet offers numerous opportunities to commit these acts, and it is extremely difficult to eliminate them due to the fact that they are one of the most complicated conducts to deal with.

12.2.1.1 Scenario

Trade-mark abuse is the action of a third party to make the most of the prestige of a brand by forging it, or making associations to it.

Most commonly, the objectives of this brand abuse are lucrative ones, making the most of a brand in an illegitimate way (for example to gain more trust or recognition within the market for their own interests) and with the aim of creating problems regarding the brand's reputation (for example by wearing out the competitors).

On the internet, trade-mark abuse has the same definition, but it differs in the way in which it occurs. All of these acts of trade-mark abuse can be produced by means of telephones, social media, apps or merchandising.

For example, it is common to find a range of apps on IOS and Android online stores which simulate being the official app of a clothing brand or well-known restaurant. This too is the case for the thousands of copies of games which, making the most of their original download, the brand is used to launch unauthorised apps.

The problem when analysing the ambit of the application of this cyber-behaviour is the main topic of debate regarding cyber trade-mark abuse: where do the limits lie? Is it considered trade-mark abuse to use hashtags on Twitter with the name of a brand? And what about creating fan pages or groups on Facebook for a basketball team using their badge and official images? The debate could be ended by arguing that commercial uses are strictly forbidden, whilst non-commercial uses are allowed. However in cyber-space the line between what is commercial and what is not is far thinner. For example, if a blog is accessed for free, but it creates income from advertising revenues and it attracts clients due to its content about car brands - is that a commercial use?

Example of Brand cyber-abuse on Twitter.
Source: twitter.com

And so, for cyber-organisations and citizens, cyber trade-mark abuse has become a hot topic for discussion and each change or development in digital devices, along with the expansion of the internet, lead to new issues.

12.2.1.2 Analysis

Just as with cyber-piracy, in the territorial world the cyber trade-mark abuse has been commonplace on the internet for some time now, and as such there are specific laws in place against this behaviour.

Whilst conducts regarding intellectual property and copyright appear in sections of different Criminal Codes, the regulations vary according to the territory, with this being a heterogeneous behaviour.

For example, in **Honduras**, this is regulated in sections 248 and 253 of the Criminal Code and under heading VI of the Decree No. 12-99-E (Law on Industrial Property),

which establish that the fraudulent use or imitation of registered brands over the internet can be sanctioned with 3 to 6 years imprisonment if it is carried out:

- By a third party
- Without the owner's consent

In **Spain**, on the other hand, these conducts that are carried out by third parties and infringe industrial property rights are regulated in the Criminal Code. Punishments are established for anyone who, knowing the situation of a registered brand and without the consent of the owner, reproduces, imitates, modifies or usurps a distinctive sign which is either identical or similar to one of the brand's, in order to distinguish itself or its products, services, activities or establishments. The sentences in this case oscillate between 6 months and 2 years of prison and the fine between 12 and 24 months.

In cyber-space, all of the organisations analysed prohibit trade-mark abuse one way or another, generally in an explicit way. For example on **Line** the Terms and Conditions prohibit any kind of activity that infringes or violates any patent, copyright, trade-mark or privacy or publicity right or any other intellectual property right that a person or entity may have. **Pinterest,** in terms of its brand policy, discloses that any content of profile which infringes or violates someone else's brand will be permanently suspended. This expressly prohibits the behaviour.

A last example is that of **Steam**, which in its Terms and Conditions which are actually called the "Subscriber Agreement**"**, establishes that "any type of use of a brand without the license owner's consent is not permitted".

All of these obligations that users have to not publish content which is subject to intellectual property rights, are formulated in the same precise and explicit way, and they are practically all complimented by online forms which are available to formally report these behaviours, these are separate to those which have the purpose of reporting other cyber-incidents.

12.2.1.3 Proposed solutions

With the aim of exploring the starting point for possible legal pathways, and to help to lead the way for others to come on board and collaborate in the search for better solutions, my proposal is based on three courses of action.

States can carry out a whole range of measures that encourage the disappearance of this cyber-behaviour, and by means of extension, of cyber-piracy too, such as for example:

- **Reporting mechanisms:** Making official channels available for cyber-organisations and citizens that need support to report a cyber trade-mark abuse or cyber-piracy.
- **Persecution:** Surveillance of the means by which trade-mark abuse and the piracy of content are available. The closure of fraudulent websites and the penalisation of piracy activities.
- **Means:** Providing the necessary means to the organisations and organisations which are in charge of carrying out these activities and of protecting industrial and intellectual property.

Example of the closing of a website in the USA.
Source: Google Images

From the point of view of **the organisations** which own the brands that are being violated, the following measures can be put in place:

- **Precaution:** the necessary precautions must be taken in order to avoid the brand or contents being copied, such as the registering with official bodies, the creation of social media accounts in the first place, and the protection of names and designs, etc.
- **Contacting the offenders:** try to peacefully request that the offender discontinues the actions that constitute abuse.
- **Contacting the regulatory authorities and bodies:** if direct contact does not work, the authorities that deal with intellectual and industrial property should be turned to so that the corresponding procedure in terms of investigating the cyber-incident can be initiated.
- **Reporting online:** on websites where these infractions take place, reports should be made via the channel made for such reason.
- **Informative campaigns about the infraction:** publicising to the media and to those that buy the "stolen" good, using the message to strengthen the image of the original brand or product.

The individual perspective in this case is focused on the **author/owner** of the rights that have been violated. These are the measures that can be adopted:

- **Precaution, contacting the offenders** and **contacting the regulatory authorities and bodies:** just in the same regard as the organisations.

- **Reporting online:** on websites where these infractions take place, reports should be made via the channel made for such reason.

12.3 Cyber Domain Abuse: Cyber-squatting

Internet addresses, such as www.ciberderecho.com, are called domain names and tend to be used to identify web sites. These make up the base of internet surfing and also suffer from antisocial cyber-behaviour, in this case: cyber domain abuse.

12.3.1.1 Scenario

Cyber-occupation, or cyber-squatting, is the registering of a domain name whilst knowing that somebody else holds more right to it. The aim being to pressure them into buying it, or to redirect traffic which was aimed for the original site, taking advantage of the brands good reputation, for example.

In summary, this involves registering a domain name with the knowledge that there is already a brand interested in it, to then sell it, extort the brand or make economic gains due to confused users trying to get to the authentic page, and this way attracting users to the web site.

Anticipation is a vital element for this conduct as cyber-squatting exists once the brand exists but before they wish to enter the online market and open their own web site.

The cyber-occupiers make the most of the fact that the system of registering domain names works on a strictly first come first serve basis, and names of brands, personalities and companies are registered which have no relation whatsoever. Given that registering names is relatively simple, cyber-squatters can register hundreds of these names as domain names.

With the ownership of these domains, cyber-squatters can auction or sell the domains directly to the interested company or person, at a far higher cost than that of registering.

Another frequent technique is that of registering domains with common words. The reasoning behind this is that sooner or later somebody will want to use one of these for their website, for example car.com or pizza.com. Domains with spelling mistakes also tend to be registered, making the most of traffic that was aiming for one site but incorrectly entered the address in the browser, for example googel.com or gooogle.com.

One last example of the actions of cyber-occupiers is that they periodically go through the lists of recently expired domain names with the aim of re-selling the domain name to the previous owner who inadvertently let the domain name expire.

Cyber-squatting is a behaviour will purely exists in the cyber-world, but with residual components in the physical world, such as with the procurement processing of the domain, however this on an increasingly more frequent scale this all takes place in cyber-space.

12.3.1.2 Proposed solutions

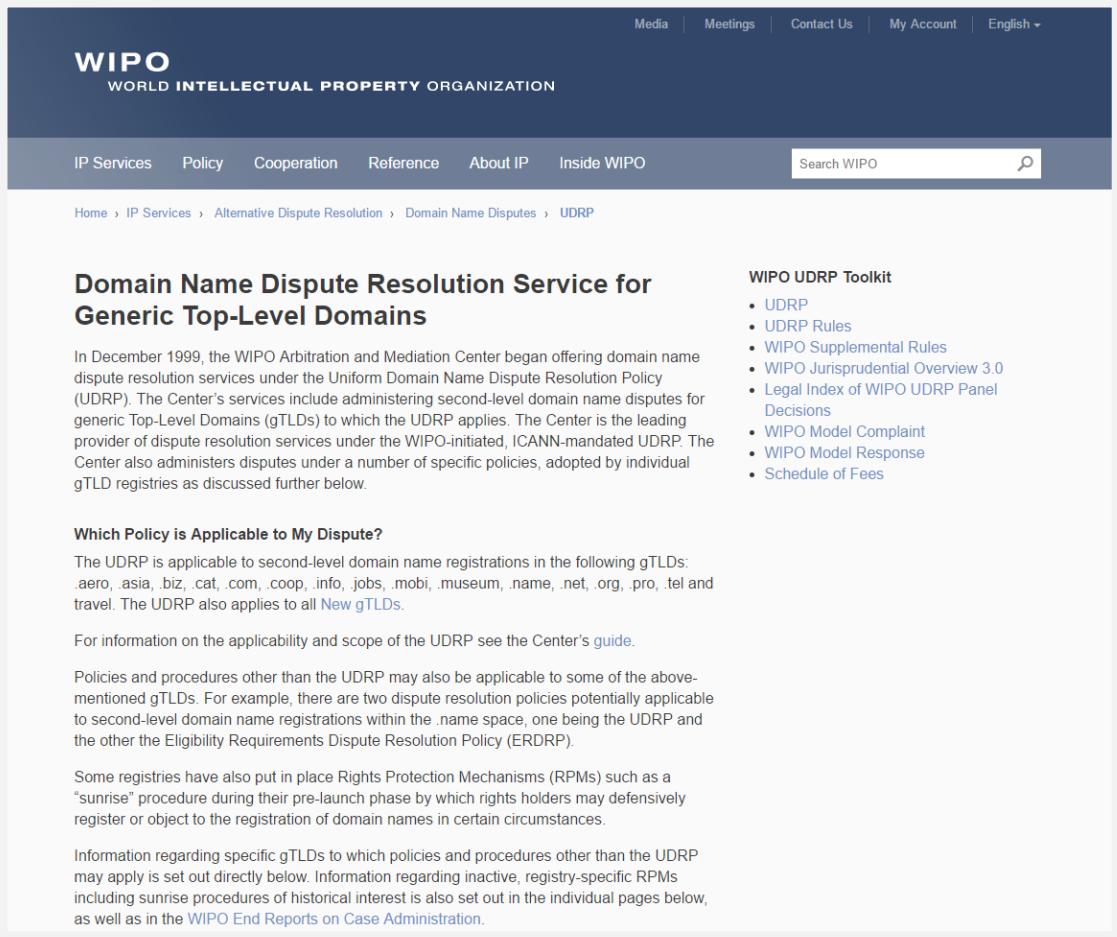
When up against the problem of cyber-squatting, the following positions can be taken with the aim of protecting a domain name that is associated with a brand:

- Judicial: Application of the legislative framework in each territory.
- Extrajudicial: application of the ICANN's policy, which is the international non-profit organisation which supervises the system for registering domain names. https://www.icann.org/es

In this regard, it is interesting to turn to the last of these; the extrajudicial solving of conflicts, above all because their resolutions apply on a global level, and they have a considerably high rate of effectiveness.

On 24 October 1999 the ICANN approved a regulation, which was later modified in 2009, which contained a uniformed policy on the settlement of disputes regarding domain names. And so, many providers of dispute settlement services can be found:

- World Intellectual Property Organization (WPIO)



One of the bodies that resolves domain name conflicts.
Source: http://www.wipo.int/amc/en/domains/gtld/

- National Arbitration Forum (NAF) (Minneapolis-St Paul)
- Asian Domain Name Dispute Resolution Centre (ADNDRC) Beijing and Hong Kong
- The Czech Arbitration Court Arbitration Center for Internet Disputes
- Arab Center for Domain Name Dispute Resolution (ACDR)

13 Anonymity in Cyber-Space

The internet that we know these days, which we have been using intensively on a daily basis for more than 15 years, is subject to a pillar which is quite possibly the most frequent cause of many of the cyber-problems that we have been analysing up till now, or it does at least facilitate their existence.

That is, of course, the anonymity in cyber-space, or in other words the capacity that users have to hide their identity and even cover the traces of their internet activities.

The tools which internet users currently have, as well as the way in which the internet is configured allows users to surf on 90% of web pages without leaving a trace which allows for their location to be identified, or to identify who is hiding behind the keyboard or device that carries out the actions.

It is true, however, that for some time elements have appeared which seek to eliminate this characteristic. For example, the need to physically identify oneself in order to carry out certain formalities, as is the case for certain procedures with the Spanish Public Administration which require the National Identity Document (DNI per its Spanish acronym).

Example of tools and websites where anonymity is the key element.
Source: Google Images

Likewise it is also true that identifying the IP address may be an element which eliminates this anonymity by defect in cyber-space, whereby the service providers (ISP) can identify a physical place in a territory as the origin of certain communications, providing that there is a legal order which warrants this.

However, these are limited mechanisms and they alone cannot fight against a system which is integrally designed with the aim of being anonymous. Despite efforts from States and organisations to combat this, more and more elements are brought out on a daily basis which continues to reinforce this principle.

The debate over anonymity on the internet has been around for years among the main discussion forums regarding the internet. Presumably it will continue to be present, with discussions such as privacy versus security, or control versus freedom of speech.

However, the inevitable pathway is possible in the near future whereby this feature is removed in favour of increasing internet security and the guarantees of users, cyber-organisations and States all at the same time.

14 The Internet of Things.

What is meant by the Internet of Things (IOTs)?

Although there is not a single definition of the internet of things, generally it refers to the digital inter-connection of everyday objects (coffee makers, heating systems, street lights, etc.) or to those situations in which the network capacity is extended to objects, sensors and everyday objects that are not normally considered as computers, allowing them to create, exchange or consume information with minimal human intervention.

There are numerous and unquestionable advantages that go hand in hand with the Internet of Things (it makes life easier, it propels the economy, it improves processes, etc.), the other side of the coin cannot be forgotten: those aspect that are yet to be improved and that users should not be left out when using them.

What are some of the cyber-problems or legal challenges that we find with the IOTs?

1. **Lack of cyber-security.** The principle of *Security by Design* is still not widespread, meaning that when a device that connects to the internet is designed (such as an activity monitoring bracelet, a video surveillance camera, or a home heating system) security is not a priority.

   In fact, there are studies which show that it is possible to enter a Home Network Installation, which is connected by WiFi, by means of an intelligent light bulb system. With the data extracted, it can be predicted when the family are going to be at home or not, which puts our security and that of our assets in danger, should said information be used with malicious intentions.

2. **Loss of privacy and data protection.** The *Privacy by Design* principle is not very widespread yet either. This involves keeping people's privacy in mind when developing the software for a device.

   Through wearables, SmartTvs, or car navigation systems with internet access, a great deal of personal data is collected. Without strict policies regarding personal privacy, all of this information can be used for a different means to that which it was collected for. This could involve an invasion of privacy and a breach of the user's data protection. For example, a third party can find out about the health of another user and use that information against them, confidential or compromising conversations can be spied on, and an individual's privacy can be violated as they exact location is known thanks to the car's GPS.

3. **Non-consented remote control.** The lack of knowledge about what "being connected to the internet" involves means that people are not aware about how vulnerable the devices are that are connected to the net and that transmit our information. A poor defect authentication, and not changing passwords, tends to be one of the key weaknesses.

   This can give way to situations such as: an energy bill being manipulated (i. e. controlling a house's heating system), damage being produced in electronic

devices (i.e. manipulating its working from the control panel), or the extracting of information about personal habits (i.e. accessing the data from a wearable*)*.

4. **The need for adapting regulations in each country and adopting standards.** For their part, companies that want to use IoT solutions will have to adapt the devices to the regulations of each country they are to be used in, adhering to standards and, at all times, the regulations regarding privacy, data protection and security of information.

5. **Offensive cyber-industry**. More and more often the so-called "intelligent factories", 4.0 industry or cyber-industries are turned to because of the advantages they hold. However, not investing in a strong cyber-security system can lead to the non-authorised access to the cyber-factory and the subsequent modifying of industrial processes, which can have catastrophic consequences. For example, through such access, a country's energy production could be paralysed.

DAILY NEWS 24/01/2015

This week, the *Wired* technology magazine has shown how some artificial intelligence systems which are already applied in the market can be an easy target for #cybercriminals. In this case, they demonstrated how you can #hack the system of an intelligent car (not an autonomous one) to interfere in its systems and boycott the driver and passengers.

In the publication's official channel's video, it can be seen how the magazine's editor-in-chief, Andy Greenburg, was attacked by just two hackers, armed with nothing but a couple of laptops and their home's internet connection, while he drove on a real motorway. Whilst connected to the network, the vehicle's braking system, sound system, air conditioning, door locks and even the steering wheel (in this last case, only very slowly and in reverse) were attacked. This all left the driver completely incapable of carrying out any action to stop the #cyberattack.

This was a test which, according to the authors, was carried out by using a special software, with the aim of discovering the vulnerabilities in these types of systems and therefore improving the security of the future updates of these products. The test was carried out on a 2014 Jeep Cherokee, but it could be applied to many other makes and models that also use systems that are connected to the internet.
As Ciberderecho has been insisting for a long time, for example in the article regarding drones http://www.ciberderecho.com/drones-los-ciberproblemas-que-sufriran/ every device that is connected to the web can suffer from a #hacking attack and their most basic system can be compromised, or they can suffer from information being stolen, #cyberespionage attacks, and other, even more dangerous, consequences.

Thanks to these types of tests, developers can improve the cyber-security of systems meaning that in the not-so-distant future the hackers will be incapable of evading the security of the online systems of intelligent cars, and thus, drivers will be protected from this type of threats.

15 Proposed solutions

15.1 Cyber-Law: A New Discipline?

To what extent does the internet create new opportunities for us? Are we seeing the beginning of a new legal discipline? Are technological advances opening the doors to a new concept of Law?

The conclusions that I have come to are that the internet is causing a revolution in our society which brings us into a new era and it is even changing the concept of Law that was understood around the world. Cyberspace is a reality that is here to stay. Thousands of millions of machines, internet users, companies and all types of organisations live within it. Who is missing? States and Governments.

This is where **Cyber-law** steps in: a discipline that studies the problems that arise regarding those that want to enter this virtual space, but it also tries to apply traditional measures and processes. A new environment has been created, one that needs to be regulated, and a new relation with the physical world has also been created which is calling for it to proceed with its legal ordering.

Cyber-law should encompass the study of the relationship between these two worlds, and it should open the debate regarding the future solutions that should be provided from either side of the wall which separates these worlds.

I invite you to reflect about this new discipline and join in the discussion that is happening on the key legal and technological forums. Cyber-law is the subject of the future and I am sure that it will become one of the great disciplines of Law in a very short period of time.

"Cyber-space disrupts usual lawmaking practice. It is not the Law that governs the internet, but the internet that governs the Law."

15.2 Proposed Global Solutions

As I introduced at the beginning of this manual, on a global scale when facing these cyber-problems and issues that emerge with Cyber-law, my proposed solution revolves around the creation of an internet protocol, together with the recognition of this new discipline.

From the perspective of the recognition of this new dimension, of Cyber-space, where the legal assets to be protected and regulated in this world are similar, but not equal, to those in the real world (domains, cyber-privacy, virtual money, cyber-brands). The regulation of this world and the new assets should be carried out with a new, distinct focus which takes these realities into account.

The legal ordering of Cyber-space (which is a mammoth task) involves the creation of cyber-rules which are applicable to cyber-citizens and cyber-organisations.

The answer to those critics that advocate for legal rules on the internet not to exist, because the internet was born free and thus it should stay free of any type of censuring,

must be that they are well within their right to think like that, but, this ideology implicitly entails that there is a "right" which is freedom, and that value is in itself a form of legal regulation.

But enjoyment of this most praiseworthy right is disrupted when a user invades your privacy and, for example, publishes private photos or steals someone else's Bitcoins. Right now there is a conflict about where the freedom of both start and end.

And for those that also have the very valid opinion that States should not be given the power to regulate the internet as they spy on us and the State is a bad public body which aims at censuring the Internet; it has to be said that I advocate for the ordering of cyber-space, but the State does not have to be the only legitimate body which can approve regulations. Quite the opposite actually, as it stands I do not know the exact formula, and I hope that other professionals provide contributions in the search for the regulatory Holy Grail of the internet. But in the meantime, I champion the passing of regulations with the consensus of many agents (States, organisations, citizens and groups of legitimate interests) and the voting of the majority of them in the search of the majority consensus and stability for a period of time.

With the creation of these cyber-regulations, cyber-courts should also be formed to resolve antisocial conducts and to proceed with the penalising of their perpetrators.

But these penalties need to been cyber-penalties and they should not pass into the real world. In the real world there are already applicable jurisdiction and laws.

And last of all, a large part of the solution lies in the creation of an IP identification protocol, as I mentioned before, which would be required in commercial and peaceful internet surfing traffic.

The internet protocol that I suggest, which I could be referred to as "ID Protocol" and that, just like the other ensemble of internet protocols, should be embedded in its own TCP/IP protocol with the aim of rectifying a large part of the problems caused by antisocial behaviour on the internet and which are difficult to prosecute, mainly because they are committed anonymously.

Just as in the physical world, he who does not have identification paperwork can freely circulate, but they cannot interact with organisations that require said identification.

Therefore, the greatest sanction for a perpetrator is to deprive them of the freedom to surf the internet, with the apprehension of their ID for a determined period of time.

Between the degree of freedom and the ID imprisonment, a scalable regime of penalties or sanctions can be established, according to the legal violation that has been infringed.

Logically, the cyber-citizen will still be able to surf the internet, even after the penalty, but they will do so in an irregular way. Just as in those countries that brought in driving licenses with points, those that do not have any points can drive, but without a regular license, and they must face the consequences if they are stopped by security forces.

In conclusion: a new democratic regulation in cyber-space with cyber-regulations, cyber-courts and cyber-penalties, with the aim of ordering the cybernetic world and establishing some rules of the game so that safer, more stable internet surfing is possible.
It is true that complete security does not exist, every activity has an associated risk; mine is putting myself on the line by proposing new ways of studying law in Cyber-space.

And so, using the syllogism of the Matrix: *How is this world different from the one that has been put before your eyes?* What is real or simulated? *What are the differences between the law put in front of your eyes and the law in cyber-space*? *What is real or virtual*?

"Welcome to the new world of cybernetic law".