# ROAR Manual

From understanding and preventing cybercrime to supporting and empowering victims

ROAR
empoderamento às vítimas de cibercrime

APAV
associação portuguesa de Apoio à Vítima

This Manual was funded by the European Union's Internal Security Fund– Police

Promoted by:
Associação Portuguesa de Apoio à Vítima (APAV) | Portugal

Partners:
Ministério da Administração Interna (MAI) | Portugal
Procuradoria-Geral da República (PGR) | Portugal
PT Portugal | Portugal
Weisser Ring | Germany
ACTEDO | Romania

ISBN: 978-989-54855-8-1
Legal Deposit:

Title:
ROAR Manual - From understanding and preventing cybercrime to supporting and empowering victims



Address:
APAV – Associação Portuguesa de Apoio à Vítima
Rua José Estêvão, 135 A
1150-201 Lisboa
Portugal

Tel.: +351 213 587 900
Email: apav.sede@apav.pt
Website: www.apav.pt
Facebook: www.facebook.com/APAV.Portugal

# CONTENTS

# CONTENTS

# PART I
# UNDERSTANDING

# PART I

# UNDERSTANDING

# 1. CYBERCRIME: A CONCEPTUALISATION APPROACH

## 1.1. Information and communication technologies [ICT] and the emergence of cybercrime

HIGHLIGHT | STATISTICS IN FOCUS:

According to EUROSTAT[1], in 2017, 87% of households in the European Union had access to the Internet, an increase of 17% in comparison with the 70% rate of 2010.

More than 85% of people surveyed reported using the Internet daily. The highest usage shares were identified in Italy, Denmark, Malta, the Netherlands and Sweden.

EUROSTAT also looked at the use of the Internet by companies and organisations: only 3% of businesses in the European Union did not have the Internet in 2017, and the largest proportions of non-use were found in Romania and Greece.

In the same survey, EUROSTAT measured some e-commerce[2] indicators: in the last 10 years, online shopping has increased for Internet users of all ages, with particular emphasis on young people between 16 and 24 years of age. Also, the survey of companies and organisations reported that 20% of businesses conducted e-commerce in 2017.

The above data (and other sources) show the increasing use of the Internet, particularly in the European Union, at various levels. They also reiterate that the Internet is indeed and increasingly, global, instantaneous, intrinsically cross-border, providing a decentralised network structure and enabling the digital presentation of information (Koops, 2010).

The Internet and Information and Communication Technologies (ICT)[3] have also facilitated, because of these same characteristics, varied opportunities for crime, modifying and increasing the possibilities of crime, either because they are in themselves potential targets of crime, or because they can also provide the means or tools through which other crimes can be committed (Van Wilsem, 2011).

It can therefore be said that the Internet has provided **new forms and opportunities to offend or commit crimes that can be designated as 'conventional'**, such as stalking, child sexual abuse or fraud, but it has also leveraged the **emergence of new forms of crime** exclusively associated with the use of computers, ICT and computer systems, such as hacking, DDoS and malware, which will be detailed in the following sections of this Handbook (Yucedal, 2010; Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

In more detail, the resources provided by the Internet, viewed as 'transformative keys', have **revolutionised the way crime can be committed** (Wall, 2007 *cit in* Jahankhani et al., 2014). We are referring, to the following features promoted or enabled by the Internet:

- **Globalisation**: cyberspace offers new opportunities to exceed conventional limits;
- **Distributed networks**: they generate new opportunities for victimisation;

[1] *Digital economy & society in the EU – A browse through our online world in figures | 2018 edition*, available at https://ec.europa.eu/eurostat/cache/infographs/ict/index.html.

[2] The world wide web allows people from all over the world to engage in commercial activities, without time and space limitations. The term e-commerce can be defined as a statistical tool to calculate transactions of goods and services on the Internet or as an information system that provides product catalogs on the Internet (Poong, Zaman & Talha, 2006).

[3] Information and Communication Technologies (ICT) refers to all technical means used to process information and assist communication, including computer hardware and networks and software.

- **Sinopticism and panopticism**: they strengthen the possibility that potential victims can be monitored online;
- **Data trails**: they create new opportunities to commit cybercrime.

Moreover, the Internet has led to the emergence of a set of online environments in which cybercrime can take place. These are:

- The ***surface web*** (websites, computers or other devices accessible and connected to the Internet);
- The ***deep web*** (websites not searchable on the surface web; intranets and medical databases);
- The ***dark web*** (subtset of the deep web that constitutes an attractive platform for the initiation and development of illegal activities).

(Maimon & Louderback, 2019).

In this 'ecosystem', we can identify the interaction of the following agents or actors, whose respective behaviour can lead to cybercrime:

- **Cyber-criminal**;
- **Enablers** – those who support the illegitimate activities of cybercrime, such as programmers and coders[4] who develop malicious software[5] (malware[6]), distributors and vendors who sell/supply tools that allow the practice of cybercrime.
- **Targets**;
- **Guardians** – police authorities and system administrators.

## 1.2. From cybercrime definitions to typologies

In this section of the Handbook we present possible definitions for the concept of cybercrime, and, for a better understanding of this phenomenon, we also use different typologies and categorisations to demonstrate its complexity and the range of forms or types of acts included.

The **concept of cybercrime** was initially designated as 'computer crime', and it covered all crimes using computers or other similar devices, including networks and other means of access. They referred, therefore, to all kinds of **attacks against the availability, integrity and confidentiality of computer systems, information systems and resources that support them** (hardware[7]) (Gouveia, 2016 *cit in* Maia, Nunes, Caridade, Sani, Estrada, Nogueira, Fernandes & Afonso, 2016).

The increasing use of the Internet and ICT has accelerated the emergence of other computer crimes that extend beyond the aforementioned attack on the availability, integrity and confidentiality of computer systems.

This leads to the adoption of concepts similar to computer crime, such as cybercrime, e-crime, digital crime and online crime.

[4] Coders are individuals dedicated to producing code, testing it and running it on a server.

[5] Software refers to abstract instruction sequences of a program, which describe calculations to be performed on a computing device (Councill & Heineman, 2001).

[6] Malware refers to malicious software designed to illicitly infiltrate other people's computer systems in order to cause damage, alterations and/or misuse of (confidential or otherwise) information/data.

[7] The internal *hardware* parts of a computer are usually called components (hard disks and RAM), while external *hardware* devices are usually called peripherals (monitors, keyboards, printers and *scanners*).

From this wider perspective, cybercrime can also be defined as a **crime in which the computer network is a *target* or a substantial *tool*** (Koops, 2010). In line with the European Commission's definition (2007)[8], cybercrime includes crimes committed using electronic communication networks and information systems and crimes against such networks and systems.

Given the nature of cybercrime and the complexity of this concept, several authors propose typologies or categorisations in order to better understand its scope and the multiplicity of associated phenomena.

Cybercrime can thus be categorised into:

- **Cyber-dependent crimes** - associated with new forms of crime, the occurrence of which depends on the existence and use of ICT, computers and computer networks (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019).

- **Cyber-enabled crimes** - traditional forms of crime in which ICT plays an important role, it includs financially motivated crime, but also forms of interpersonal violence and sex crimes. Examples are cyberstalking or Internet scams (Leukfeldt et al., 2020), which we will address below.

This categorisation of cybercrime distinguishes cyber-dependent crime from crime made possible by the Internet and ICT. In the latter case, the different forms of cybercrime that are made possible or enabled by the Internet and ICT can in turn be further subdivided into:

- Financially motivated cybercrimes (e.g. phishing[9] and romance scams[10]);
- Cybercrimes in interpersonal relationships (e.g. cyberstalking);
- Sexual cybercrimes (e.g. revenge porn[11]).

To the above categorisation, others may be added, such as those summarised in the following table.

[8] See Communication from the Commission to the European Parliament, the Council and the Committee of the Regions: *Towards a general policy on the fight against cybercrime*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14560&from=PT.

[9] Additional information on this phenomenon is given in Part I, section 1.3 of this Handbook.

[10] Additional information on this phenomenon is given in Part I, section 1.3 of this Handbook.

[11] Additional information on this phenomenon is given in Part I, section 1.3 of this Handbook.

**Table I-1: Types and Categories of Cybercrime**

| | |
|---|---|
| Wall, 2005 *cit in* Reep-van den Bergh & Junger, 2018 | **Crimes against computers**: pertain to the unauthorised access to the boundaries of computer systems, such as hacking/cracking[12], where the computers are the focus/target of the attack (e.g. computer viruses);<br><br>**Crimes using computers**: where ICT are used to commit crime (e.g. identity theft and the fraudulent online use of credit cards);<br><br>**Crimes 'in' computers**, where the criminal content is the crime (e.g. online child sexual abuse and/or exploitation material, threats of violence and terrorism). |
| Jahankhani et al., 2014 | **Computer as the target**: for example, theft of property, illicit access to information (e.g. customer list) and its use to obtain other benefits, including financial, through threat;<br><br>**Computer as the instrumentality of the crime**: for example, fraudulent use of card and bank account information, conversion or transfer accounts, credit card fraud;<br><br>**Computer is incidental to other crimes**: for example, money laundering and unlawful banking transactions;<br><br>**Crime associated with the prevalence of computers**: software piracy, copyright violation of computer programs, equipment/program counterfeiting and theft of technological equipment. |
| Yar, 2006 *cit in* Jahankhani et al., 2014 | **Cyber- trespass**: the crossing of cyber boundaries of computer systems, causing damage to property rights or ownership (e.g. hacking);<br><br>**Cyber-deceptions and thefts**: fraudulent use of credit cards and (cyber) cash through raiding of online bank account and e-banking;<br><br>**Cyber-pornography**;<br><br>**Cyber-violence**, which includes cyberstalking and online hate-speech;<br><br>**Crimes against the state**, encompassing online activities that breach laws which protect the integrity of the state, such as terrorism, espionage, and disclosure of official secrets. |

HIGHLIGHT | INFORMATION IN FOCUS:

Despite these and other categorisations, there is no universal conceptualisation of the different types of cybercrime. From the previous typologies, it can be roughly deduced that cybercrime can be organised into:

- Cybercrime against computers and computer systems;
- Cybercrime enabled or practiced through computers and computer systems.

One can also conclude that, in dealing with cybercrime, we are in fact referring to **a set of diverse crimes** involving computer systems and computers as instruments either for committing crime or as targets.

[12] Additional information on this phenomenon is given in Part I, section 1.3 of this Handbook.

## 1.3. The different types of cybercrime: current trends

In the following sections of this Handbook, we present a brief overview of the currently considered main phenomena (or, at least, the phenomena that deserve greater prominence or concern) in the area of cybercrime. It should be noted, however, that cybercrime and its various forms, including the contexts in which they occur, the tools they use and/or their targets, are constantly changing, and it is possible to include other types of cybercrime not covered in this section of the Handbook.

It is also important to note that, despite growing knowledge about the various phenomena of cybercrime, information about the real scale of victimisation by different types of cybercrime is still incipient, and therefore the real prevalence rates in the population are unknown (Reep-van den Bergh & Junger, 2018). Wherever possible, the following sections cover data from official cybercrime statistics, criminal victimisation surveys and/or other studies that somehow make it possible to measure the size of the different types of cybercrime, particularly at the European level.

HIGHLIGHT | STATISTICS IN FOCUS:

The study by Reep-van den Bergh and Junger (2018) sought, through the analysis of different victimisation surveys, to find a rough estimate of the prevalence of cybercrime in Europe.

Some of the main results are summarised below:

- Between 0.6% and 3.5% of the population reported being victims of **online shopping fraud** and, among the cyber-victimisation situations identified, approximately 90% concerned the purchasing of goods or services, paid but not received.
- The prevalence rates of **online banking fraud and payment** range from 0.4% to 2.2%.
- About 3% of the population reported having experienced some form of **cyberbullying**, including threatening behaviour, with a proportion ranging from 0.6% to 1.0%, and stalking in similar proportions (0.7% to 1.1%).
- As far as cybercrime is concerned, despite the ranges, **hacking** and **malware** were identified as forms of cyber-victimisation with a higher prevalence: between 1.2% and 5.8% of the population reported being victims of hacking and between 2% and 15% reported being targeted by malware.

The study is available at: Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science, 7*: 1-15.

The types of cybercrime mentioned above, as well as others, will be addressed below.

However, it is also important to contextualise the fragilities associated with the measurement of cybercrime: the general population's lack of knowledge about the different forms of cybercrime, which may lead

to an underestimation of cybercrime effectively experienced and reported to the authorities, and the devaluation of some of the cybercrime phenomena, are among different aspects that compromise knowing the real dimension of cybercrime (Maimon & Louderback, 2019).

### 1.3.1. *Hacking and Cracking*

**Hacking** or **cracking** is commonly defined as **unauthorised access to computer systems with criminal intent** (Grabosky, 2016 *cit in* Maimon & Louderback, 2019). They are associated with cyber-trespassing, which involves the unauthorised crossing of invisible boundaries of online environments (Wall, 2001 *cit in* Maimon & Louderback, 2019).

Hacking includes a number of behaviours, such as **redesigning hardware or software systems** to change their intended function, as well as participating in the hacker subculture (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019). This activity has multiple stages, which may include: identification and reconnaissance of vulnerable hardware or software systems; infiltration of vulnerable targets; changes and redesign of target systems, including installing viruses and malware allowing privileged access to information and data (such as personal data, passwords/access credentials and financial information/bank accounts) or even the control over the system itself; cover up of the intrusion and of the system modifications (Hughes & Delone, 2007, Wolfe et al, 2008, Holz et al., 2009, Waldrop, 2016, Luo & Liao, 2009 *cit in* Maimon & Louderback, 2019; Jahankhani et al., 2014).

Like most **cybercrimes**, hacking also **mediates the practice of other cybercrimes**, serving as a means for other illicit acts to be possible and successful, such as the hacking of an e-mail account in cyberstalking situations (Leukfeldt et al., 2006 *cit in* Leukfeldt et al., 2020) and a DDoS (distributed denial-of-service attack).

With regard to hacking, differentiated classifications of hackers are also proposed, according to their intention (Furnell, 2002 *cit in* Maimon & Louderback, 2019):

- **White hat hackers** (hackers whose unauthorised access to systems is intended to increase those systems' security);
- **Black hat hackers** (hackers who unauthorisedly access systems with illicit intent).

There is also a conceptual differentiation that should be addressed: the classification of black hat hackers is close to the concept of **cracker**, that is someone who, unlike the white hat hacker, takes advantage of their knowledge and unauthorised access to computer systems to use the information and data at their disposal for illicit purposes and/or for the purpose of obtaining personal advantage or benefit.

### 1.3.2. *Spamming, Malware* and *DDoS* [distributed denial-of-service attack]

**Spamming** or **SPAM**, the acronym for 'Sending and Posting Advertisement in Mass', refers to the **sending of data and mass distribution** of e-mails advertising products, services or investment schemes, which may be fraudulent and even contain malware or other executable file attachments (Rathi & Pareek, 2013).

Spam meets three criteria:

- Anonymity - the address and identity of the sender are concealed or missing;
- Mass distribution - the email is sent to a large group of people/electronic addresses;
- Unsolicited – the e-mail is not requested by recipients (Rathi & Pareek, 2013).

Spam's purpose is to deceive or persuade the recipient to engage with attractive products, services or schemes. The sender may request cash or security information, such as credit card number or other personal information, before the supposed access to the products or services occurs (Jahankhani et al, 2014).

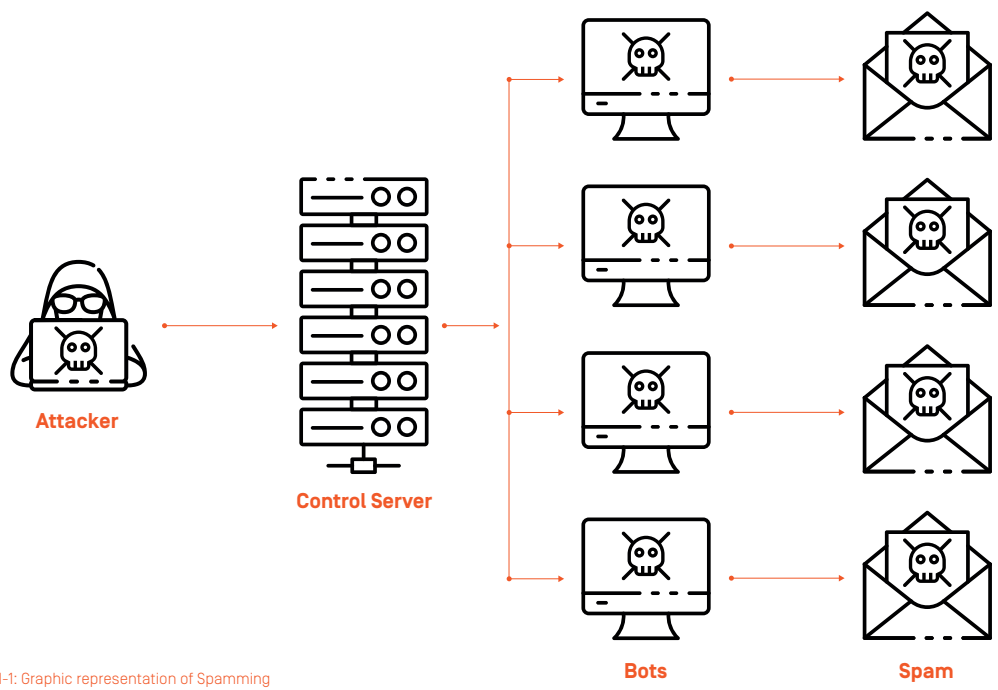


Figura I-1: Graphic representation of Spamming

**Malware** refers to a variety of hostile or intrusive software (e.g. computer viruses, worms[13], ransomware[14], spyware[15], adware[16], scareware[17], etc.).

This is **software intended to infiltrate equipment illicitly** in order to cause damage, alterations or theft of information. Malware can also take the form of executable code, scripts, active content and other software (Aycock, 2006 *cit in* Reep-van den Bergh & Junger, 2018).

A frequently used scheme is the publication of content with titles that arouse curiosity or call for some kind of 'urgent' action, as well as invitations to install games or suggestions to visit new profiles.

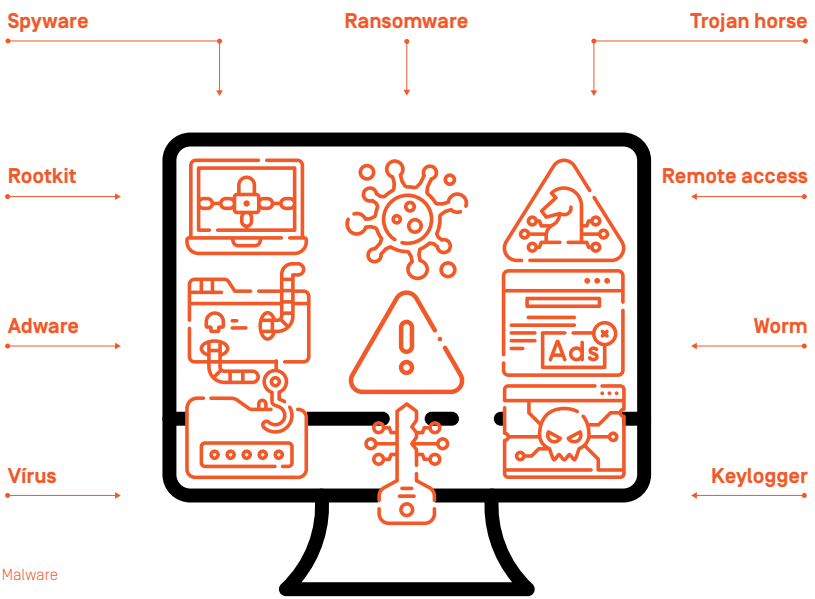


Figure I-2: Types of Malware

The **distributed denial-of-service (DDoS) attack**, in its turn, concerns an intentional attempt to overload a particular computer system (such as that of government structures or large companies, for example), with the purpose of making it unusable (Overvest & Straathof, 2015). The most common form of a DDoS attack is through the use of a Botnet. A Botnet is a network of bots (computer zombies) managed by a botmaster (hacker) through a commanding server, that coordinates and controls the access to all devices connected to the network. The instalment of a Botnet is dependant on a prior infection of the computer system, usually by malware.

[13] Worms are malicious codes that spread through a network, with or without human assistance (Kienzle & Elder, 2003).

[14] Ransomware is malware inserted into the system by download and that creates an 'exe' file to run. The goal may include the extortion of the victim by encrypting their personal information (Kansagra, Kumhar & Jha, 2016).

[15] Spyware is an automatic program that collects information about the user and their Internet usage habits and transmits this information to an external entity, without the user's knowledge and consent.

[16] Adware is software that automatically displays or downloads (usually unwanted) advertising material when the user is online (Gao, Li, Kong, Bissyandé & Klein, 2019).

[17] Scareware is a form of malware that fools the user into believing that their computer is infected when in fact the system is working (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).

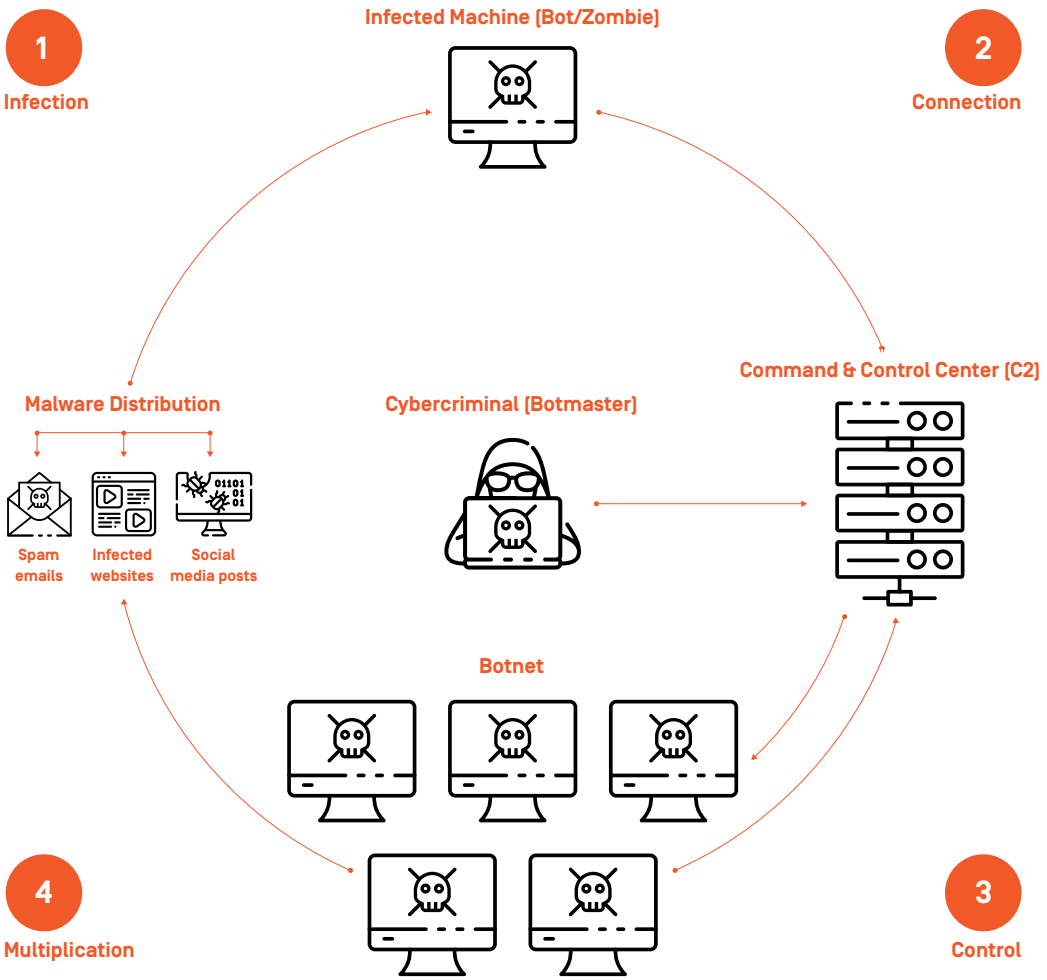


Figure I-3: Graphic representation of how a Botnet works

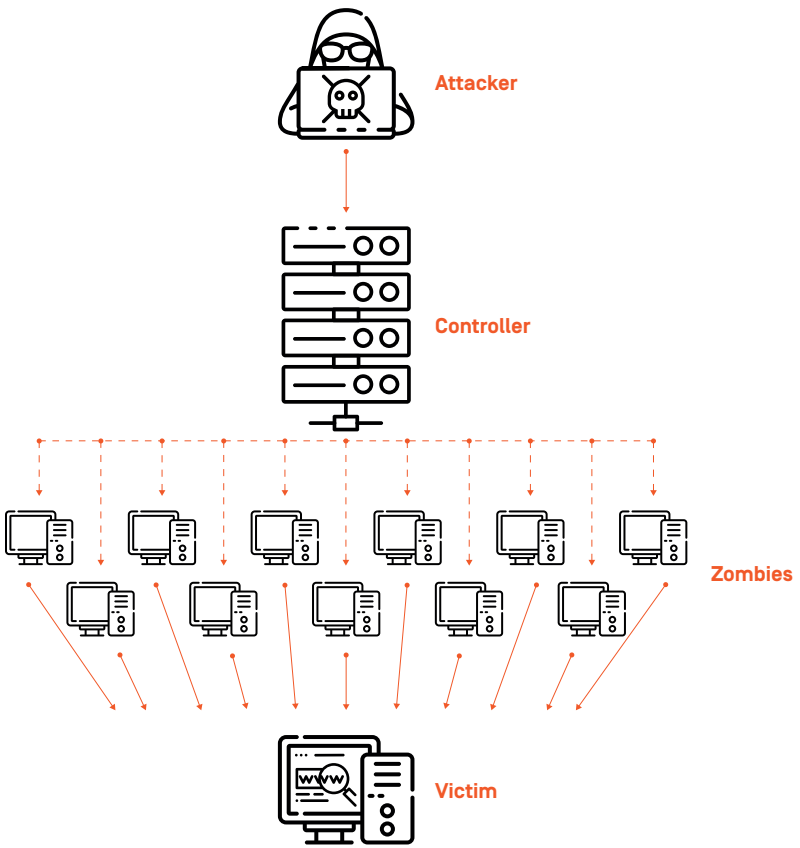


Figure I-4: : Graphic representation of a DDoS attack[18]

### 1.3.3. Online fraud

#### 1.3.3.1. Online shopping fraud

Online shopping is characterised by the inability to physically inspect the items, goods or products before purchase, and by the lack of direct contact between the parties involved in the buying and selling process (Moons, 2013, van Wilsem, 2013 *cit in* Reep-van den Bergh & Junger, 2018), increasing the risk of online shopping fraud.

[18] Imagem de https://pt.safetydetectives.com/blog/o-que-e-um-ataque-ddos-e-como-se-prevenir/

Online shopping fraud presents **different degrees of complexity**, from simple schemes, in which the seller promises to send the buyer a certain article after a bank transfer is made, and the latter not receiving the said article (or receiving a different article from the one that has been acquired). Fraud can also entail more elaborate schemes that often involve the falsification of documents, such as proofs of bank transfers.

In terms of frauds and their practices, there is also the possibility of exploiting vulnerabilities in online shopping websites that store users' bank details (such as credit or debit card details), which are illegally accessed and then sold by cyber-criminals on the dark web or used for bank transactions without the victims' knowledge (**card not present fraud**). The theft of users' bank details for this type of fraud usually occurs through phishing, a phenomenon explored in the following sections of this Handbook.

#### 1.3.3.2. Internet auction fraud

**Internet auction fraud** is another type of fraud that occurs when the purchased items are fake products or obtained by illicit means or when the seller advertises nonexistent items or makes them available for sale. In this type of fraud, it is usual to use bank transfer services to enable the transaction of money without the need to reveal the identity of the parties involved (Jahankhani et al., 2014).

Auction fraud relies on anonymity and sometimes also on the use of false identification data when registering on the auctions' platforms or websites.

Some of the most common situations include:

- Acquisition/purchase of goods that are not received by buyers;
- Paid and received goods that do not correspond to the desired goods (e.g. the good received is significantly different from the original description/photo);
- Non-disclosure or incomplete disclosure of relevant information about the item and/or the terms of sale;
- No payment received by sellers.

#### 1.3.3.3. Credit card fraud

**Credit card fraud** refers to the **use of another person's credit card for personal use, without the card owner's and the issuer's knowledge** (Patel & Singh, 2013). There are several cyber-dependent methods/crimes that can be used to obtain access to these cards and their details, such as phishing, spamming or hacking (Jahankhani et al., 2014).

In the scope of **credit card fraud**, one should highlight **skimming fraud**, which consists of copying

the magnetic strip of a payment card without the knowledge or consent of the cardholder, when they use that card at an ATM (automated teller machine) or at a till point terminal. After the copy of the magnetic strip of the paymenr card, the data might be transmitted to other parts of the globe, enabling payments/money withdraws in those locations.

Recently there have been other types of attacks, notably on ATM machines, in a process called **jackpotting**. The attack to ATM machines can occur through the introduction of malware in the computer system of the equipment/ATM or through hardware connection, called 'Black-Box'. Then the criminal gives the command for the ATM machines to dispense the cash they have.

#### 1.3.3.4. Online romance and dating scams

Scams in intimate relationships occur when the agent seeks to establish a **relationship of trust and intimacy**, particularly through the Internet and ICT, with a certain target, as a prelude to **personal benefit, namely financial and patrimonial benefit**.

This form of fraud usually includes:

- Creating false profiles on social networks, dating sites or other chat and social interaction platforms;
- Establishing contact with apparently more vulnerable targets;
- Creating an emotional bond with the previously identified target;
- Developing a narrative with the intention of extorting personal/financial assets from the target.

This process of courting and creating a relationship with the victim aims to gain access to their money or other assets, bank accounts, credit cards, passports, e-mail accounts and/or personal identification numbers. It may also aim to coerce the victim into committing crimes on behalf of the perpetrator.

### 1.3.4. Online identity theft

Identity theft covers the **unauthorised obtaining of personal and/or confidential data** from a specific victim (such as name, personal identification number, credit card number, etc.), and its **possession or transfer** and **use** in committing a crime.

It includes the following cumulative acts:

- Obtaining personal and/or confidential information about another person without their knowledge;
- Possession or transfer of such data knowing that they will be used for illicit purposes;
- Use of previously obtained data for committing crimes.

These acts correspond to **online identity theft** when the personal and/or confidential data of the victim are obtained through the Internet, and/or when the data obtained, by any means, are transferred through the Internet, and/or these data are used to commit a crime through the Internet.

Its objectives are usually to obtain financial advantage, credit and other benefits, to create disadvantage or loss for the victim (Enisa, 2010, Harrell & Lagton, 2013, Tuli & Juneja, 2015 *cit in* Reep-van den Bergh & Junger, 2018) and even to commit crimes on behalf of the victim. The victim whose identity has been used, in addition to financial losses, may thus be subject to legal consequences if they are held responsible for the perpetrator's actions.

Identity theft does not constitute a crime in itself but may, otherwise, encompass a variety of crimes foreseen and punishable under the Portuguese Penal Code.

### 1.3.5. Phishing

Phishing translates into the mass sending of e-mails - spamming - usually with a link to a web page that recipients are persuaded to access and appealing to urgent reasons or actions.

As a rule, these e-mails either request or highlight the importance of the recipients 'updating', 'validating' or 'confirming' banking information.

These e-mails (and the pages to which they refer) are false and constitute an approximate reproduction of the original communications made by banks, credit institutions or others that allow online payments.

When accessing such pages, the user is usually asked to enter banking information, making thus possible for the criminal to capture and misuse it.

Thus, phishing encompasses different illicit acts (Jahankhani et al., 2014) and different stages:

- Setting up a **false web site/page**, which mimics a reliable website of a reputable or trustworthy organisation, usually a banking organisation. This webiste or page includes a *login* or registration form and can also redirect to the actual website or page of the aggrieved banking organisation, after using the form.
- Creating a fake e-mail that, just like the web site/page, mimics the reputable or trustworthy organisation's communications and **calls for urgent action on the part of the recipient** (e.g. warning that customers need to log in immediately to prevent the blocking or inactivation of accounts/access data), with subsequent **spamming**.
- **Obtaining personal and/or confidential information** from the recipient, including banking details, through their access to the link.
- **Misuse** by the crime perpetrator of the banking details obtained for economic benefit and/or for the commission of other crimes.

HIGHLIGHT | STATISTICS IN FOCUS:

According to Eurobarometer 423[19], which analysed EU citizens' perceptions about Internet use, cyber-security and cybercrime, 68% of people surveyed are concerned about **online identity theft**, followed, in decreasing order, by concern about malicious software/malware (66%), **online fraud**, namely bank card fraud (63%), and **hacking** of their e-mail accounts and social networks (60%).

In addition, 47% of respondents reported having already been the target of **malware** and 31% reported having already been the victim of **phishing** attempts.

### 1.3.6. Sexual abuse and exploitation of children via the Internet

Child sexual abuse is defined by the World Health Organization - WHO (2017) as the involvement of a child, i.e. any person under the age of 18 years, in sexual activity:

- that the child does not fully comprehend;
- for which the child is unable to give informed consent to, or is not developmentally prepared for consenting to;
- that violates laws or social taboos of society.

Different types of child sexual abuse can be considered (WHO, 2017):

- **Non-contact sexual abuse**, which includes threats of sexual abuse, sexual harassment, grooming, sexual solicitation, exposure of the child to pornographic content/materials, among other forms of abuse that do not involve direct contact between the victim and the offender;
- **Contact sexual abuse**, which includes, for example, the practice of vaginal, anal and/or oral sex with the child, through penises, body parts or objects, as well as other sexual acts such as inappropriate kissing, fondling and touching.

The increasing and earlier **use of the Internet and social networks** by children, combined with reduced, non-existent and/or inefficient family supervision, increases their **exposure to sexual abuse and exploitation through the Internet** (Council of Europe, 2007 *cit in* APAV, 2019; Livingston & Smith, 2014).

[19] Additional and detailed information about this Eurobarometer - Special Eurobarometer 423: Cyber security - is available at https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

HIGHLIGHT | STATISTICS IN FOCUS:

According to INTERPOL's[20] *International Child Sexual Exploitation* (ICSE) database, more than 1.5 million images and videos were recorded in 2018 and 19,400 children were identified as victims of sexual abuse and exploitation worldwide.

Following a random selection of videos and images from the aforementioned ICSE database, INTERPOL and ECPAT International published a joint report entitled *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material in* 2018, and we highlight the following results:

- 92% of visible offenders were male;
- 65% of unidentified victims were girls;
- More than 60% of unidentified victims were prepubescent, including babies and toddlers;
- The younger the victim, the more severe the abuse;
- 84% of images contained explicit child sexual abuse content, including explicit sexual activity.

Some forms of child sexual abuse and exploitation via the Internet are addressed below[21].

#### 1.3.6.1. Online child sexual abuse

Online sexual abuse, as a comprehensive concept, can be defined as encompassing **any form of child sexual abuse in an online context**, which includes different manifestations, from non-contact sexual abuse facilitated by ICT and the Internet, social networks or other platforms, such as harassment and grooming, to sharing content on the dark web (image and/or audio) of child sexual abuse and exploitation, using previously taken photographies or video.

#### 1.3.6.2. Online child sexual exploitation

The concept of child sexual exploitation is distinguished from other forms of abuse as it is characterised by extraction, gain and benefit arising from the subjection of the child to some type of sexual act. It is difficult to clearly dissociate it from the concept of sexual abuse but, as a rule, sexual exploitation involves exploiting a child's characteristic, situation or condition, and the benefits are collected by the perpetrator, third parties or even the child themselves (as is the case, for example, of the child subjected to situations of sexual abuse in exchange for love and affection by significant adults).

**Online child sexual exploitation** includes all acts of a sexual nature with an ICT connection committed against a child, such as:

- Sexual exploitation carried out while the child victim is using the Internet and ICT, including the

[20] Additional and detailed information is available at https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[21] For detailed information on terminology and different forms of child sexual abuse and exploitation, please see the EPCAT International and EPCAT Luxembourg Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse, available at http://luxembourgguidelines.org/english-version/.

seduction, manipulation and threat of the child to perform sexual acts before a webcam, for example;
- Identifying and/or grooming potential victims online for sexual exploitation (regardless of whether the exploitation and abuse takes place online or offline);
- Distribution, disclosure, import, export, offer, sale, possession or conscious online access to child sexual exploitation materials (even if the sexual abuse content contained in the material was performed offline).

#### 1.3.6.3. Live online child sexual abuse

This phenomenon involves the **practice of sexual acts with children and their transmission live**, through live streaming services, thus making it possible for them to be watched by other people. The viewing may imply the prior payment of a certain amount, and spectators may even have the possibility of dictating or defining the course of the acts of sexual abuse and exploitation practiced against the child.

Live streaming means that data are transmitted instantly and with less risk, since it does not require the download of any file and, as soon as the transmission is interrupted, the material disappears, making it difficult to investigate the crime, collect evidence and identify victims and perpetrators.

Live child sexual abuse involves different forms of child sexual abuse and exploitation, including the production and distribution of child sexual abuse and exploitation materials and prostitution. It represents a **twofold form of child sexual victimisation**: first, the child is forced or, in some way, led to participate in sexual activities, alone or with other people; simultaneously, the sexual activity is transmitted live, through ICT, and viewed remotely by other people.

#### 1.3.6.4. Online grooming

Online grooming can be defined as a **process of manipulation** and a **form of solicitation** of children. It usually starts with a non-sexual approach through the Internet and ICT, including online games and social networks, in order to establish a relationship of trust with the child and to convince the child to meet face-to-face so that the perpetrator can consummate the sexual abuse. The establishment of a relationship of trust with the child, mediated by the Internet and ICT, may also aim to persuade the child to produce and share sexual content[22].

Online grooming allows offenders to select the type of victim they want to manipulate and entice. In addition, online grooming allows the enticement of a large number of victims simultaneously, among other advantages for the perpetrator, such as anonymity, preserving their real identity and managing their other 'identities' with which they present themselves to the selected targets.

As a result of this form of sexual abuse and exploitation, the offender may subject the child to threats

[22] In the context of self-generated sexual content, we may include, by way of example, sexting, as a form of self-production of content - text, images and/or videos - of a sexual nature and its sharing, usually in a consensual manner and among peers. However, it may be produced under pressure or coercion or even lead to the non-consensual sharing of the content produced.

and blackmail to disseminate or share the self-generated sexual content, with the aim of attracting sexual favours, money or other benefits. This phenomenon is called **child sexual extortion**.

HIGHLIGHT | PRACTICES IN FOCUS:

*Childline*[23] is a free, confidential service made available specifically to children and young people in the UK, addressing a wide range of issues and problems that can affect these age groups.

Among several topics, the service has information on safe behaviour in the use of the Internet and ICT, as well as an online mechanism for reporting the sharing/dissemination of self-produced sexual content.

The reporting mechanism is available at: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/.

#### 1.3.6.5. Online child sexual abuse and exploitation material [CSAM/CSEM]

HIGHLIGHT | STATISTICS IN FOCUS:

According to the already mentioned Eurobarometer 423, 7% of the people surveyed reported having been accidentally exposed to **online child abuse and exploitation material**.

The expressions **child sexual abuse material** and **child sexual exploitation material** (CSAM/CSEM) seek to replace, at least in non-legal contexts, the concept of child pornography (terminology still featuring in national and international legislation), and cover:

- In the case of child sexual abuse material, the content and material that represents or depicts acts of sexual abuse of children and/or children's sexual organs;
- In the case of child sexual exploitation material, as a more comprehensive terminology, all material that portrays or represents children in a sexualised manner.

This change in terminology is based on the argument that any material representing a child in a sexualised way is in fact a form of child sexual abuse and child sexual exploitation and should not be described as 'pornography'.

**Child sexual abuse and exploitation material generated digitally or by computer**, whether in whole or in part, is also considered child sexual abuse and exploitation material.

[23] Detailed additional information is available at: https://www.childline.org.uk/.

### 1.3.7. Cyberbullying, cyberstalking and other forms of online aggression in interpersonal relationships

Bullying is a phenomenon of peer violence that implies or involves the perpetration of aggressive and violent behavior by an aggressor or group of aggressors against a victim or group of victims with the goal of hurting them, causing them harm or suffering (APAV, 2011).

**Cyberbullying** involves the use of ICT and the Internet, with the aim of verbally assaulting the victim and/or contributing to their exclusion and social isolation. Some of the behaviours that are included in this form of online aggression are: the dissemination of negative/false information with the intention of defaming the victim (by using phone calls, text messages, video messages, e-mail, chat room, websites, social networks); harassing the victim (by using the same means) (APAV, 2011; Jahankhani et al., 2014).

Cyberbullying is distinguished from more conventional forms of bullying by the possibility of being done at any time of the day, regardless of the need for direct contact between victim and aggressor; the potential for anonymity of the aggressor; the high potential for 'advertising' and audiences (it can be infinitely shared on social networks or any other Internet communication platform where it was initiated/published and even between platforms); and the difficulty of removing the content created[24].

HIGHLIGHT | STATISTICS IN FOCUS:

According to the results of the EU KIDS ONLINE[25] survey, involving 19 European Union countries, on the use of the Internet and online practices and experiences of children between 9 and 16 years of age, on average 5% of children reported being **cyberbullied** during the last 12 months before the survey.

Still in the same survey, about 22% of the participating children reported having already received **messages with sexual content**. See previous sections, in which different forms of child sexual abuse and exploitation via the Internet are addressed.

According to the latest data from the transnational *Health Behaviour in School-aged Children*[26] study, conducted regularly by the World Health Organization (WHO), the prevalence of **cyberbullying** is higher than that identified in the previous survey: respectively, 12% and 14% of male and female adolescents reported having experienced cyberbullying.

As far as the different forms of cyberbullying are concerned, we can highlight the following online aggression behaviours with a sexual nature:

- Online sharing of rumours or lies about the victim's sexual behaviour;
- The online use of offensive or discriminatory sexual language directed against the victim;
- Identity theft aimed at sharing sexual content and/or sexual harassment against others using

[24] Additional information at https://www.stopbullying.gov/.

[25] Detailed additional information on the study is available at Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online. Doi: 10.21953/lse.47fdeqj01ofo.

[26] Detailed additional information is available in the reporto f the study: WHO (2020). *Spotlight on adolescent health and well-being: Findings from the 2017/2018 Health Behaviour in School-aged Children (HBSC) survey in Europe and Canada - International report*. Copenhagen: WHO Regional Office for Europe.

the victim's identity;
- Online sharing of information regarding the victim's intimacy, in a non-consensual manner, as a strategy to perpetuate large-scale assault and harassment behaviours.

We could also add *body shamming* via the Internet and ICT, which involves sharing derogatory comments about the victim's physical appearance, and *outing*, when someone reveals (or threatens to reveal) publicly, via the Internet and ICT, information about the victim's sexual orientation or gender identity without their knowledge and permission.

**Cyberstalking** can be defined as a form of stalking which, while still intrusive, repetitive and persistent and causing fear to the victim (characterics of this form of persecution and persistent harassment), is practiced using the Internet and ICT with the aim of threatening and harassing the victim (Maran & Begotti, 2019).

Cyberstalking practices may include different predatory behaviours: making several unwanted attempts to contact the victim, via telephone, e-mail and social networks; installing spyware on the victim's computer; accessing the victim's e-mail and/or social network accounts without the victim's authorisation, to monitor private information and the daily life of the victim and/or to act using their identities (Martellozzo & Jane, 2017).

Cyberstalking can precede the practice of other forms of stalking in conventional contexts or even take place as part of a stalking and harassment campaign that takes place both online and offline. Offenders can be people the victim knows, including friends and co-workers, as well as ex-partners or unknown people (Maran & Begotti, 2019).

HIGHLIGHT | STATISTICS IN FOCUS:

According to a European survey on violence against women[27], over 40,000 women surveyed in the different Member States of the European Union, with 5% reporting having been the victim of some form of **cyberstalking** since the age of 15.

The Member States that stood out were Sweden, with the highest prevalence at 14%, and, Spain with the lowest prevalence at 2%.

In what concerns online violence in interpersonal relationships, we can highlight, in addition to cyberbullying and cyberstalking, the **non-consensual disclosure of images and videos** – this pertains to sharing intimate images, including photographs, films and/or video recordings, without the consent of the person who has their nudity, body parts, including sexual organs, and/or sexual activity exposed.

The motivations for disclosing this content can include:

[27] Detailed additional information on the results of the *European Union Agency for Fundamental Rights'* European survey is available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

- **Sexual extortion or coercion of the victim**, in which the perpetrator, after receiving from the victim, usually in a consensual manner, videos and/or photographs of a sexual nature, threatens disseminating them if the victim does not provide new self-generated content of a sexual nature or does not agree meeting the aggressor face-to-face.

- **Revenge**, often referred to as revenge porn, involves the non-consensual disclosure of intimate images - photographs, films and/or video recordings of a partner, usually after the relationship has ended, as a form of retaliation. This is a common phenomenon in the field of violence in intimate relationships where, following the relationship breakdown, sexual images and/or videos of the former partner are disseminated (or there are threaths to disseminate them), to family and friends, through social networks or even on pornographic websites.

HIGHLIGHT | PRACTICES IN FOCUS:

Facebook offers, in *Not Without My Consent*, a range of information resources associated with sexual extortion and the non-consensual dissemination of images and videos.

*Not Without My Consent* also has a space for reporting non-consensual sharing/dissemination of images and videos, as well as a guide with instructions for removing online content.

Detailed additional information is available at: https://www.facebook.com/safety/notwithoutmyconsent.

### 1.3.8. Other forms of cybercrime

**Cyberterrorism** is a form of terrorism that uses information, computers, networks, and technical infrastructures to conduct terrorist activities. Because of the importance of these interconnecting network components, cyberterrorism could be considered potentially more harmful than *traditional* terrorism. In particular, cyberterrorism targets financial and business infrastructures, as well as government infrastructures, air traffic control, and medical records, with the advantage that it can be accomplished with modest financial resources, anonymity, and at a distance (Hansen, Lowry, Meservy & McDonald, 2007).

The intent of cyberterrorism is to **incapacitate and/or drastically reduce the availability of the computing resources of an organisation, entity or infrastructure**: for a private company, this type of attack may result in financial losses; for a government entity, it may lead to the inability to fulfill its mission (Kratchman, Smith & Smith, 2008).

The concept of cyberterrorism is associated with the destruction and/or incapacitation of **critical infrastructures**, which, if compromised, can have a debilitating impact on national security, economy and the social situation of a given country (Dunn & Wigert, 2004 *cit in* Yar & Steinmetz, 2019). Within

these critical infrastructures, we could include communications, energy, water, food, emergency services and health services, as well as symbols of national cohesion (Milone, 2003 *cit in idem*). Among these infrastructures, those in the information and telecommunications sectors stand out for their central role in the functioning of a country's other critical infrastructures (Dunn & Wigert, 2004 *cit in idem*).

For the practice of cyberterrorism, several of the cyber-dependent crimes mentioned throughout this Handbook can be committed.

On another note, we could include **online hate speech**, which includes all forms of communication and expression, through the Internet and ICT, that promote, disseminate, incite or seek to justify racial hatred, xenophobia, anti-Semitism and other forms of hatred based on intolerance against a person or group of people.

HIGHLIGHT | STATISTICS IN FOCUS:

In *Flash Eurobarometer 469 - June 2018*[28] , respondents were asked about the type of illegal content accidentally encountered online. Among several options, **hate speech** was the most mentioned type of illegal content in 10 countries, particularly in Malta (55%), the Czech Republic (53%), Bulgaria (52%) and Poland (50%).

Respondents who reported having viewed at least one type of illegal content online were asked about their actions:

- The majority (59%) stated they had not taken any action after viewing the illegal content.
- Among the actions carried out, the most common was informing the Internet Service Provider (21%).
- About one in ten people surveyed directly contacted the person or entity responsible for the content (9%) or alerted the police/authorities (8%).

The growing use of the Internet, ICT and social networks has been accompanied by the proliferation of **online hate speech against certain groups of people** (Banks, 2010 *cit in* Martellozzo & Jane, 2017). This proliferation is based on a set of characteristics associated with the Internet and ICT, of which we can highlight (Yar & Steinmetz, 2019):

- It is a low cost and efficient tool, based on a low financial investment, with the capacity to disseminate hate speech to wide audiences;
- It presents less risk of detection and identification, by enabling anonymity and preservation of the identity;
- It allows access to communication channels that would not be available otherwise for the dissemination of this type of discourse;
- It allows the content and format of information transmission to be adapted according to the audience and target groups.

[28] Detailed additional information is available at https://ec.europa.eu/digital-single-market/en/news/flash-eurobarometer-illegal-content.

HIGHLIGHT | PRACTICES IN FOCUS:

In May 2016, the European Commission and four digital platforms (Facebook, Youtube, Twitter and Microsoft) announced a **Code of Conduct against Hate Speech Online**[29], to which other companies have adhered.

One of the goals of this code is the more immediate removal of online hate speech content, namely within 24 hours, with the purpose of reducing its audience reach.

## 1.4. The dark figures of cybercrime

The cybercrime numbers that we have been summarising throughout the previous sections of this handbook do not portray, despite their expressiveness and significant dimension, the cybercrime's effective reality.

The precise cybercrime prevalence is unknown. It is likely to be a **larger number of undetectable, unreported, uninvestigated and unresolved cybercrimes**, given the invisibility and complexity of the digital evidence associated with its occurrence, eventual legislation gaps, and even cybercrime's transnational nature (Koops, 2010; Cangemi, 2004 cit in Yucedal, 2010).

Additionally, the widespread reluctance of cybercrime victims to report (Koops, 2010), either out of fear, ignorance and/or devaluation of the acts they have been subjected to, also contributes significantly to the lack of knowledge about cybercrime's real magnitude.

There are several explanations for the non reporting of cybercrime and, consequently, for the gap between the numbers of cybercrime that comes to the attention of the competent authorities and the 'real' cybercrime (Goucher, 2010; Kanayamaa, 2017; Maimon & Louderback, 2019; Leukfeldt et al., 2020), of which we highlight:

- The cybercrime victims' lack of knowledge or recognition of the acts they have been subjected to as forms of crime;
- Feelings of shame, guilt and blame for their cyber-victimisation;
- Devaluing of damages and losses caused by cybercrime;
- The victims' reluctance or resistance of reporting cybercrime to the competent authorities;
- The failure to identify benefits associated with reporting cybercrime to the competent authorities, given the potential failure of cybercrime investigations and the apparent limited damage caused by cybercrime (at least in terms of the damage and impacts felt/ perceived by each individual victim);
- The lack of familiarity and knowledge of cybercrime;

[29] The Code of Conduct and additional information on its creation and implementation are available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1135 .

- The lack of cybercrime specific training for all security forces and the lack of financial resources for further research;
- The absence of specific or specialised support services or responses, differentiated from traditional responses to victims of 'conventional' crime, which could assist the victim of cybercrime in obtaining help/linking to available resources;
- The lack of accessible systems and mechanisms (in particular through the Internet) and simple reporting of cybercrime.

Acknowledging the existing difficulties, we highlight throughout this Handbook examples of responses, services and existing mechanisms, which underline the efforts made to promote and facilitate access to support services, information, as well as online mechanisms for reporting cybercrime.

HIGHLIGHT | PRACTICES IN FOCUS:

AEUROPOL - *European Union Agency for Law Enforcement Cooperation* offers on its website a page where it is possible to access the cybercrime reporting mechanisms (including online reporting where applicable) existing in different Member States.

This page is available at: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online.

HIGHLIGHT | PRACTICES IN FOCUS:

*Action Fraud* is the UK's national complaints centre for online scams and other cybercrimes.

In addition to the telephone support provided, *Action Fraud* provides an online reporting tool, accessible at: https://reporting.actionfraud.police.uk/login .

In the case of **sexual abuse and exploitation of children via the Internet**, other obstacles are associated with the disclosure of the child's experience of victimisation, such as:

- Feelings of guilt and shame for the cyber-victimisation they experienced;
- A feeling of (self-)responsibility due to the victim's perception that they were, in some way, complicit or conniving with the cyber-victimization situation;
- Fear of reprisals by the cybercrime perpetrator and/or punishment by those legally responsible in case of disclosure;
- Fear of being discredited;
- Fear of losing rewards that they may receive from the perpetrator of acts of sexual abuse and ex-

ploitation in return for the practice, participation and/or production of sexual content;
- Failure to identify situations of sexual abuse and exploitation as unlawful acts and/or interpret them as manifestations of affection.

(Goodman-Brown, Edelstein, Goodman, Jones, & Gordon, 2003 *cit in* Sigurjonsdottir, 2013; Berelowitz et al., 2012; Martellozzo & Jane, 2017; APAV, 2019).

HIGHLIGHT | PRACTICES IN FOCUS:

INHOPE[30] is a network currently made up of 46 *hotlines* from various countries, including the Member States of the European Union, aimed at combating online child sexual abuse and exploitation material.

The Portuguese Association for Victim Support (APAV) is responsible, in **Portugal**, for the operation of the Safe Internet Line [*Linha Internet Segura*], under the consortium Safe Internet Centre [Centro Internet Segura], promoted by the Foundation for Science and Technology. In addition to providing support and information on Internet safety issues, the *Linha Internet Segura's* intervention includes a platform that allows and facilitates the **anonymous reporting of illegal content on the Internet**, with emphasis on online child sexual abuse and exploitation material and incitement and promotion of racism, xenophobia and other forms of violence.

The reporting platform is available at: https://www.internetsegura.pt/.

In **Germany**, the *Safer Internet Center* [31] is also a platform that provides safety information about using the Internet to families, children and young people and to teachers. It also includes telephone helplines and a platform for reporting online child sexual abuse and exploitation material: https://www.jugendschutz.net/hotline/.

In **Romania**, one of the countries that is also part of INHOPE, the Save the Children Romania has available an electronic mechanism/form that facilitates the reporting of illegal online content. See: https://oradenet.salvaticopiii.ro/esc-abuz

With regard to **cybercrime against collective entities**, namely organisations and companies, whether small or large, studies indicate a high cybercrime prevalence, particularly of **cyber-dependent crimes** (Rantala, 2008 *cit in* Maimon & Louderback, 2019; Saini, Rao & Panda, 2012). Paradoxically, the rates of reporting identified are quite low, which may be associated, among other reasons, to:

- The fear of compromising the entity's reputation, its public image and/or the brand, products and/or services it provides;
- Fear of losing the trust of the society and of citizens in the entity's activity and in its quality and reliability;
- The minimisation of possible financial losses associated with potential impacts on the dimensions indicated above;
- The fact that the cybercrimes were practiced by someone internal to the entity.

[30] Additional and detailed information is available at https://www.inhope.org/EN .

[31] Additional and detailed information is available at https://www.saferinternet.de/.

# 2. THE LEGAL FRAMEWORK ON CYBERCRIME

## 2.1. Cybercrime as seen by the Council of Europe

In view of the need to safeguard fundamental rights in cyberspace and protect against the heavy socio-economic consequences associated with the practice of cybercrime, the criminal regulation of unlawful conduct which has in its essence, or as a facilitating element, the use of computer means, is crucial. In this sense, the criminalisation of these conducts and their constant updating carries in itself not only a message of deterrence for possible agents of crime, but also that the fight against cybercrime is increasingly at the top of states' political agendas.[32]

The most relevant international instrument in the area of cybercrime is the Council of Europe Convention on Cybercrime of 23 November 2001, which aims at "the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation" in order to "make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form".[33] To this end, the Convention requires the signatory States to adapt their substantive and adjective domestic criminal law to the specific features of these crimes, with the aim of harmonising legislation, including appropriate procedural and evidence-gathering instruments, and simplifying international co-operation in order to facilitate and expedite detection, investigation, evidence gathering and prosecution. Finally, it also seeks the harmonization of substantive criminal law and, in order to enhance prosecution and investigation by police and judicial authorities, the Convention also suggests the implementation of specific procedural measures appropriate to this type of crime and promotes international co-operation.

Regarding protection against sexual abuse and exploitation of minors, the lead document is the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, commonly known as the Lanzarote Convention.[34] In force since 1 July 2010, it has extended criminal offences to cover all possible types of sexual offences against children. Of particular relevance in cybercrime is the typification of child grooming conducts through exposure to sexual and unlawful content related to the sexual exploitation and abuse of minors. The Convention also covers sexual abuse within the child's family or 'circle of trust', as well as acts carried out for commercial or profit purposes. Accordingly, States are urged to develop specific legislation criminalising all conduct referred to in the Convention, to investigate and prosecute the crime perpetrators, and to promote preventive measures taking into account the child's best interests. Finally, international co-operation among States is also promoted.[35]

## 2.2. Cybercrime in European Union Law

Within the European Union (EU), several instruments regarding cybercrime have been adopted. In 2013, a Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions defined the Cybersecurity Strategy of the European Union[36]. The strategy's key pillars are the harmonisation of policies and the establishment of co-operation mechanisms between Member

[32] Joint Communication to the European Parliament and the Council; Resilience, Deterrence and Defence: Building strong cybersecurity for the EU; JOIN(2017) 450 final; Brussels, 13.9.2017; pp. 2-3.

[33] Council of Europe Convention on Cybercrime, Budapest, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[34] Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97.

[35] For more information, see https://rm.coe.int/information-note-the-council-of-europe-convention-on-the-protection-of/16807962a7.

[36] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions; Cybersecurity Strategy of the European Union: An Open, Safe And Secure Cyberspace, Brussels, 7.2.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN .

States in order to ensure cybersecurity and respect for EU democratic principles. To this end, it proposes the creation of appropriate legislation on cybersecurity, aimed at developing the industrial and technological resources to ensure digital security and the creation of national units to combat cybercrime. Thus, the Communication foresees synergies with the private sector for the development of digital resilience. On the other hand, it also foresees preventive measures such as awareness campaigns and specialised training on the phenomenon. The Communication also calls for investment in scientific and technological research in order to bridge the technological gaps in Member States. Finally, the Communication defines how to react to possible cyber-intelligence attacks from third countries. Priority areas for action should be the sexual abuse of minors, fraudulent payments, botnets and unauthorised interference with computer systems.

In view of the exponential increase in cybercrime in recent years, the European Parliament adopted a resolution on the fight against cybercrime on 3 October 2017[37]. The resolution "condemns any system interference undertaken or directed by a foreign nation or its agents to disrupt the democratic process in another country". In addition, the European Parliament points out that "awareness about the risks posed by cybercrime has increased, but the precautionary measures taken by individual users, public institutions and businesses, remain wholly inadequate, primarily due to lack of knowledge and resources".

The resolution identifies the main axes in the fight against cybercrime and highlights prevention; ensuring that victims fully benefit from the rights enshrined in Directive 2012/29/EU; protection of children's rights; strengthening the responsibility of Internet Service Providers (ISP) in order to obtain higher quality products and more security; improving co-operation mechanisms between police, judicial authorities and ISP; adopting a common policy on criminal justice in cyberspace, which will in turn be crucial in obtaining and preserving electronic evidence; strengthening computer and technological capacities; increasing co-operation with third countries.

The EU is thus in a process of constant modernisation of its directives to ensure that they are kept up to date in order to combat new threats effectively. Below are listed the main binding instruments at EU level relating to cybercrime:

Regarding cybercrime *strictu sensu*;

Directive 2011/93/EU - on combating the **sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA**[38], which was created to tackle the new criminal phenomena associated with the sexual abuse and exploitation of minors, grooming and child pornography online. To this end, the Directive defines offences, penalties and aggravating circumstances, as well as minimum custodial sentences, the punishability of attempts and different forms of authorship, such as complicity, and the criminal liability of legal persons, as well as the obligation to have databases of offenders in order to prevent recidivism. Finally, the Directive urges co-operation between public and private entities in the protection, assistance and support of victims and the obligation of specialised training for all those involved in criminal proceedings. In this regard, the Directive also establishes special procedural guarantees for victims, in addition to those

[37] European Parliament Resolution of 3 October 2017 on the Fight Against Cybercrime (2017/2068 (INI)), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0366&-from=EN.

[38] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography and replacing Council Framework Decision 2004/68/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN .

already defined in the Victims' Directive[39]. Finally, it establishes the existence of preventive intervention programmes, prevention and intervention measures during or after criminal proceedings. This legislation was transposed into the national laws of the Member States in 2013. Two reports have already been prepared on the implementation of the directive by Member States in 2016.

Directive 2013/40/EU – **on attacks against information systems and replacing Council Framework Decision 2005/222/JHA**[40], aims at regulating large-scale cyber attacks so that Member States strengthen their national legislation in this area and define criminal offences and penalties for offenders as well as the criminal liability of legal persons. The Directive also aims at improving co-operation between competent authorities and Member States. This Directive was transposed into the international legal systems of the Member States in 2015.

Directive (EU) 2019/713 - **on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA**[41], this Directive is intended to complement Directive 2013/40/EU in order to cover, as criminal offences, digital conduct aimed at theft, robbery or any other form of unlawful appropriation, counterfeiting or falsification, possession or acquisition of new technological non-cash payment instruments, as well as the minimum penalties for such conduct. This new directive therefore enshrines not only infringements relating to corporeal non-cash payment instruments but also non-corporeal, as well as all electronic transactions (e.g. transactions made in virtual currency). Thus, the definition of digital means of exchange enshrined in this document includes not only electronic means of payment but also, for the first time, means of payment in virtual currency.

On the issue of obtaining and preserving digital evidence, especially in relation to illegal content;

Directive 2000/31/EC - **on electronic commerce**.[42] Among the Directive' various purposes, we highlight those concerning service providers. For the purposes of the Directive, the activity performed by the service provider is limited to the technical process of operating and opening access to a communication network in which the information provided by third parties is transmitted or temporarily stored for the sole purpose of making the transmission more efficient. Thus, the activity of the service provider is seen as a purely technical activity, automatic and of a passive nature, which implies that the information society service provider has no knowledge of or control over the information transmitted or stored.

In this sense, the Directive provides for limitations of the liability of intermediary service providers for illegal content shared by the users of the service. Thus, the service provider does not have an obligation to monitor the content and therefore cannot be held responsible for it. However, the exemption from liability is limited by a duty to act - by blocking or removing the contents - when it is aware that the recipients of its services are using it to store illegal content. In such cases, the service provider must, as soon as it becomes aware or is made aware of it, proceed with diligence to remove the information or disable access to it. The service provider is not required to actively monitor illegal content; however, it is possible for Member States to define in law the duty of care for service providers to detect and prevent certain types of illegal activity.[43]

[39] Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-%3A32012L0029

[40] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

[41] Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&-from=EN

[42] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

[43] In this matter, see also : Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334&-from=EN

Regulation 679/2016 - **Implemented the general data protection regulation (GDPR)** in 2016.[44] This new legal framework brings enhanced protections regarding personal data. It excludes from its scope the processing of information for the purpose of prevention, investigation, detection or prosecution of criminal offences by the competent authorities.[45] It therefore applies to all other situations involving the processing of personal data, in particular when detecting illegal content in the context of data processing by a service provider or other entity during the course of their activity, since detection was not the data processing purpose. The GDPR is still applicable in cases where a body or entity collects personal data in the course of its activities and then processes them in order to comply with a legal obligation,[46] for example the removal of content of sexual abuse and exploitation of minors or in the case of financial institutions when they retain, for the purpose of investigation, detection or prosecution of criminal offences, certain personal data processed by them and supply these data only to the competent national authorities.

Among the various GDPR provisions, the 'right to be forgotten', enshrined in art. 17 of this law, is given greater prominence with regard to safeguarding the rights of victims, especially when personal data are processed in an unlawful manner and therefore give rise to further harm. In this regard, there are cases of domestic violence in which images or intimate videos of a partner are disclosed without the partner's consent and made available on a pornographic site. The right to erasure allows the victim of this non-consensual dissemination of videos to demand that the platform immediately remove the illegal content.

The right to be forgotten provides its holder with the possibility to **request verbally or in writing** that the data controller deletes the personal data of the data subject. The circumstances in which this right may be exercised are described in Article 17 itself.

It is important to bear in mind that the unlawful processing of personal data, whether by the Data Protection Officer or by other persons/entities not authorised to process such data, entails criminal liability in certain cases.[47]

**EU strategy for a more effective fight against child sexual abuse**[48] – the most recent EU document on child sexual abuse and exploitation. This Communication sets out a strong and comprehensive response to these crimes, both in their online and offline form. For the purpose of combating these crimes, the strategy sets out eight initiatives to implement and develop the right legal framework, strengthen the law enforcement response and promote a coordinated multi-stakeholder action concerning prevention, investigation and assistance to victims, and defines specific action to be taken by Member States. In addition, the strategy commits the EU to the possible creation of a European centre to prevent and counter child sexual abuse, which would provide support to Member States in the fight against child sexual abuse and exploitation, ensuring utmost coordination. This strategy is to be implemented over the course of the next five years (2020-2025).

At European level, there are also institutions that have been set up to assist Member States in combating cybercrime, such as the *European Union Agency for Network and Information Security* (ENISA), which supports the exchange of good practice on cybersecurity between EU Member States. A specific

[44] Regulamento 679/2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016R0679-20160504

[45] Cf. Art. 2/2/d) GDPR. In these cases, the special regime of Directive 2016/680, transposed by Law 59/2019, will apply.

[46] Cf Art. 6/1/c) GDPR.

[47] In Portugal, criminal liability in these cases is provided for in Law 58/2019 of 8 August, Articles 46 to 52.

[48] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (COM(2020) 607 final), Brussels, 24.7.2020, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20200724_com-2020-607-commission-communication_en.pdf.

department for combating cybercrime - the European Cybercrime Centre (EC3) - was set up within Europol in 2013 to strengthen the response of law enforcement authorities within the EU. The EC3 acts by providing support to Member States' police forces in the fight against cybercrime in the EU, bringing together their experience in supporting investigations into cybercrime that may be taking place in Member States.

In addition to this initiative, the Global Alliance Against Child Sexual Abuse Online was launched in 2012 by the European Commission and the United States of America with the aim of joining efforts around the world to more effectively combat online sex crimes against children. Bringing together 54 countries, they committed to take concrete action to improve victim protection, identify and prosecute offenders, raise awareness, and reduce the spread of online child pornography and child victimisation.

At the international level it is also important to highlight the role of the INHOPE Association, whose mission is to provide support in the creation and maintenance of hotlines dedicated to combating online child sexual abuse material. These hotlines act at a national level in constant articulation with its international counterparts, in order to support structures allowing civil society to report contents of sexual abuse of minors that are available on the Internet. The hotlines' ultimate function is to lead to the removal and criminal responsibility of those who provide this type of content.

## 2.3. The legal framework for cybercrime in some Member States of the European Union

### 2.3.1. The case of Portugal

As far as Portuguese national law is concerned, the reference framework results, in the first instance, from Law 109/2009 of September 15, the *Lei do Cibercrime*, Cybercrime Law, which transposes Framework Decision 2005/222/JHA (which was replaced by Directive 2013/40/EU) and adapts domestic law to the Budapest Convention (CCCE).

This law provides for the so-called cybercrimes *strictu sensu*, that is, those whose practice depends on a computer system, and therefore *cyber-dependent offenses*. This concept of cybercrime concerns crimes that attack the availability, access, integrity, authenticity, confidentiality, conservation and security of information.

However, as we will see below, there are other crimes that can be committed using electronic means, albeit not exclusively, thus also making them part of the cybercrime phenomenon. Within these, there are also those where the law makes express reference to the use of electronic means and others, where although there is no express reference, they can still be committed using information and communication technologies (ICT).

The following tables analyse the legal types of crime provided for in articles 3 to 8 of the Cybercrime Law:

**Table I-2: Cybercrime Law**

| Article and heading | Conduct | Nature | Article of the CCCE |
|---|---|---|---|
| Article 3 - **Computer forgery** | The entering, modification, deletion or suppression of computer data with the intention of causing the deception in legal relations, or otherwise interfering with computer data processing, producing false data or documents, with the intention that they are considered or used for the relevant legal purposes as if they were true. | Public | Art. 7 |
| Article 3, paragraph 3 | To use a document produced from computer data that were the object of the acts referred to in paragraph 1 of this article, or to use a card or other device in which data that were the object of the acts referred to in paragraph 1 of this article are recorded. | | |
| Article 4 - **Damage to software or other computer data** | Delete, alter, destroy, in whole or in part, damage, remove or render unusable or inaccessible software or other computer data of others or in any way affect their ability to use, without legal permission or without being authorized by the owner, by another holder of the right to the system or part of it. | Semipublic | Art. 7 |
| Article 4, paragraph 2 | The attempt is punishable. | | |
| Article 5 - **Computer sabotage** | Hinder, impede, interrupt or seriously disrupt the operation of a computer system by entering, transmitting, deteriorating, damaging, altering, deleting, preventing access to or removal of software or other computer data or by any other form of interference with a computer system, without legal permission or without being authorized by the owner, another right holder of the system or part thereof. | Public | Art. 5 |
| Article 6 - **Unlawful access** | Accessing a computer system, without legal permission or without being authorized by the owner, by another right holder of the system or part thereof. | Semipublic | Art. 2 |
| Article 6, paragraph 5 | The attempt is punishable. | | |
| Article 7 - **Unlawfaul interception** | To intercept, by technical means, transmissions of computer data that are processed within a computer system, directed to this system or proceeding from it, without legal permission or without being authorized by the owner, by another right holder of the system or part of it. | Public | Art. 3 |
| Article 7, paragraph 2 | The attempt is punishable. | | |
| Article 8 -**Unlawful reproduction of protected program** | Reproduce, disclose or communicate, illegally, to the public, a computer program protected by law. | Public | |
| Article 8, paragraph 3 | The attempt is punishable. | | |

**Table I-3: Cybercrime Law - criminalisation of conducts of facilitation/material support to the practice of the main conduct as autonomous crimes and not as complicity**

| Article and heading | Conduct | Article of the CCCE |
|---|---|---|
| Article 3, paragraph 4 – **Computer forgery** | Import, distribute, sell or hold for commercial purposes any device that allows access to a computer system, to a payment system, to a communications system or to a conditioned access service, on which the actions prohibited by paragraph 2 of the article have been performed - enter, modify, delete or supress data recorded or incorporated in a payment card or in any other device that provides access to a payment system or means of payment, to a communications system or to a conditioned access service, producing false data or documents, with the intention that they are considered or used for relevant legal purposes as if they were true. | Art. 6, paragraph 1, als. a] and b] |
| Article 4, paragraph 3 - **Damage to software or other computer data** | Illegally produce, sell, distribute or otherwise disseminate or introduce within one or more computer systems devices, software or other computer data intended to produce the unauthorised actions described in paragraph 1 of the Article. | |
| Article 5, paragraph 2 – **Computer sabotage** | Illegally produce, sell, distribute or otherwise disseminate or introduce within one or more computer systems devices, software or other computer data intended to produce the unauthorised actions described in paragraph 1 of the Article. | |
| Article 6, paragraph 2 - **Unlawful access** | Illegally produce, sell, distribute or otherwise disseminate or introduce within one or more computer systems devices, programs, a set of executable instructions, code or other computer data intended to produce the unauthorised actions described under paragraph 1 of the Article. | |
| Article 7, paragraph 3 - **Unlawful interception** | Illegally produce, sell, distribute or otherwise disseminate or introduce within one or more computer systems devices, software or other computer data intended to produce the unauthorised actions described in paragraph 1 of the Article. | |

Some considerations should be made about the above described articles.

**Article 3**, on **computer forgery**, seeks to protect the security of legal relations as an essential public interest, which the rule of law must ensure.

It differs from computer fraud, as defined in Art. 221 of the Portuguese Penal Code, as it aims to protect the legal good. Thus, while the **legal good** protected in the former pertains to the integrity of information systems and computer data, in the latter it pertains to the patrimony. In addition, some criminalised conducts that differ from computer fraud, such as the **production of non genuine data or document with the intention of causing deception in legal relations and using the document as true**, are still required for meeting the threshold of computer forgery.

It should be noted that the article's paragraph 2 includes the falsification of computer data inserted in SIM cards (*Subscriber Identity Module*). These are plastic cards containing a chip (semiconductor structure) on which digital information is stored and allowing the holder to use a mobile phone handset to access a

mobile telephony network. The object of the conduct can also be cards or other equipment allowing access to a cable television signal, to the Internet or to telephone services – that is, 'devices enabling access to conditioned access services'.

**Example**: Phishing e-mail that forwards Josefina to a web page designed by cybercriminals and that looks like her bank's webpage in order to get Josefina to put her bank information there.

In **Article 4 - Damage related to software or other computer data**, the legislator intended to punish **unlawful actions that destroy or affect the ability to use software or computer data**. Security tests to a certain system are therefore excluded, provided they are authorised by the owner of that system.

The legal asset protected in this type of crime includes the data's integrity and reliability and the proper functioning of computer programs. Unlike the crime of damage defined in art. 212 of the Portuguese Penal Code, article 4 does not intend only to protect property – the computer damage. Thus, in addition to the patrimonial integrity of computer data as the injured party's property, this article also protects **the data's functional integrity** with regard to the **availability and effective use of computer data**. It does not require specific intent.

**Example**: João's computer is infected with a virus that makes his computer very slow.

**Article 5 - Computer sabotage** aims to protect against **disruption of computer systems** or **disruption of data communication**.

The distinction between computer damage and computer sabotage is not easy. Comparing the two types of crime, we can say that the crime of computer damage intends to punish acts related to **computer data**, while the crime of **sabotage punishes the disruption of the normal operation of computer systems**. Individually considered, we can have acts of computer damage that have, as a practical result, computer sabotage due to their impact on the functioning of a computer system or on data communication. In this case, the **damage conducts are merely forms of the crime of computer sabotage**. In other words, computer sabotage will always result in computer damage.

The provision also punishes the spread of viruses and other malicious programs designed to cause computer sabotage (e.g. art. 5, para. 2 of the Cybercrime Law). In these cases, we are criminalising the preparatory phase of the acts of sabotage, for example, the assembly of botnets intended to allow the malevolent control of networks, through the establishment of a zombie computer network whose subsequent use will cause technical failures known as DoS and DDoS.

**Article 6 - Unlawful access is** intended to protect the security and confidentiality of the computer system. This is an abstract crime of danger intended to act as a barrier to prevent the commission of other, more serious, offences. Therefore, for the typical conduct to occur, it is sufficient that **the unauthorised access is consummated**, since the knowledge of commercial or industrial secrets or

confidential data, protected by law, constitutes an aggravating circumstance of the crime of unlawful access (art. 6, no. 4 of the Cybercrime Law).

**No damage or loss to data**, programs or computer systems **is required** to consummate the crime of unlawful access. For the purposes of the law, access is the entry into all or part of a computer system (hardware, components, data stored in the system, files, traffic data and data relating to content). However, Art. 6, no. 2 does not punish the purchase/acquisition of data or programs that facilitate access, but only the sale.

For the crime to be consummated, the perpetrator is not required to have any specific intention as the mere intention to access the system suffices.

The crime of unlawful access can be committed through 1) Access carried out by exploiting weaknesses in the accessed system or 2) Access carried out by someone close to the victim (ex-boyfriend, for example), abusing the access authorisation that had been granted to him once.

**Examples**: The crime of unlawful access is committed by someone who: 1) not being authorised to do so, exploits a weakness in the system and accesses a private group in Whatsapp created by students in high school and; 2) Ana gave her boyfriend the password to, on a certain date, access her e-mail and see if an important e-mail has been received. Knowingly that he only had permission for accessing the e-mail on a specific date, he used again the password and accessed her e-mail more times.

**In Article 7 - Unlawful Interception**, the law intended to protect the right to privacy, as a right to secrecy over communications of computer data, by means of secrecy in all digital communications.

Interception authorised by law (carried out under criminal procedural rules, for example: art. 12 to 19 of the Cybercrime Law) or carried out with the authorisation or by order of those involved in the transmission of data (test or protection activities approved by the participants) are excluded from this criminal conduct.

It is a crime to intercept any form of electronic data transfer, by telephone, fax, e-mail or file. For the consummation of the crime it is **not necessary to effectively obtain information**, it is enough to act with the objective to capture this information, since the attempt to intercept is punishable.

**Example**: Pedro installs software on Maria's phone which allows him to have access to all her telephone communications.

It should be noted that the types of crime provided for in Articles 3 to 7 also include, with the same penalties, the acts of producing, selling, distributing, disseminating or introducing in a computer system a device or program that allows the practice of the criminal conduct of the crime in question. E.g.: In the case of unlawful access, someone who creates a software designed to allow a third party to access

another person's system commits the crime of unlawful access, even if he has not himself accessed or tried to access that computer system. Thus, the mere conduct of developing such software suffices.

**Article 8 - Unlawful reproduction of a protected program** aims to protect a private right, a computer program. In this sense, article 14 of DL 252/94, of 20/10, which regulates the legal protection of computer programs, expressly states that the provisions of article 9(1) of the Cybercrime Law are applicable to computer programs. It was thus understood that there was an essential interest of the State in **protecting intellectual rights of creators** and that, therefore, the interest of the State in acting criminally against the violation of rights of this nature was justified. Therefore, this crime does not depend on filling a criminal complaint, being a public crime.

Articles 11 to 19 lay down rules regarding procedural law, which allow the expeditious collection and maintenance of electronic evidence. They therefore apply to the crimes provided for in this law, those committed by means of a computer system or those requiring collecting evidence in electronic form. Articles 20 to 26 pertain to international co-operation and Article 27 to territorial jurisdiction.

**The Portuguese Penal Code and provisions on Cybercrime**

As previously mentioned, in the Portuguese legal system, in addition to the Cybercrime Law, it is also possible to find crimes that can be committed by electronic means, although not exclusively, also called cyber-enabled offenses.

In some cases, the law makes express provision for the use of such electronic means, in others it does not. In the Penal Code itself some provisions can be found that expressly refer to the use of electronic means to commit the crime. The following table gathers the provisions related to cyber-enabled offenses:

**Table I-4: Portuguese Penal Code**

| Article and heading | Conduct | Nature |
|---|---|---|
| Article 152, paragraph 2, al. b) – **Domestic Violence** | Disseminating personal data, such as images or sounds, concerning the privacy of one of the victims without their consent, via the Internet or other means of general public dissemination. | Public |
| Article 176, paragraph 1, als. a), b), c) and d) – **Pornography of minors** | To use a minor in a pornographic show or to lure them to this purpose; to use a minor in a pornographic photography, film or recording or, regardless of the medium, to lure them to this purpose; to produce, distribute, import, export, divulge, exhibit, give away or make available the materials foreseen in the previous paragraph; to acquire, hold or house those materials with the purpose of distributing, importing, exporting, divulging, exhibiting or giving away them. | Public |
| Article 176, paragraph 5 | To acquire, hold, access, obtain or facilitate access by computer system or by any other means to the materials referred to in point (b). | |
| Article 176, paragraph 6 | In person or through a computer system or any other means, to attend, facilitate or make available access to a pornographic show involving the participation of minors under 16 years of age. | |
| Article 176, paragraph 8 | Defines "pornographic material" as any material that, for sexual purposes, represents minors involved in real or simulated sexually explicit behaviour, or contains any representation of their sexual organs or other part of their body. | |
| Article 176, paragraph 9 | The attempt is punishable. | |
| Article 176 – A – **Enticing minors for sexual purposes** | Grooming of minor, through information and communication technologies, for meetings aiming at the practice of acts of sexual abuse of minors or acts of child pornography. | Public |
| Article 193º - **Intrusion by means of ICT** | Create, maintain or use a file of individually identifiable data concerning political, religious or philosophical beliefs, party or trade union membership, private life or ethnic origin. | Public |
| Article 193, paragraph 2 | The attempt is punishable. | |
| Article 221º - **Computer and communications fraud** | Interfering with the result of data processing or incorrectly structuring a computer program, using incomplete or incorrect data, using data or intervening in any way in the processing, without authorization, with the intention of obtaining for oneself or for a third party unjust enrichment, causing the other person patrimonial damage. | Semipublic |
| Article 221, paragraph 2 | To cause damage to the property of others, using programs, electronic devices or other means which, separately or together, are intended to diminish, alter or prevent, in whole or in part, the normal operation or operation of telecommunications services. | |
| Article 221, paragraph 3 | The attempt is punishable. | |
| **Crimes which, although there is no express mention of the use of electronic means, are nowadays mostly committed through them;** | | |
| Article 154 - A - **Persecution** | Persecute or harass another person, by any means, directly or indirectly, repeatedly, in a manner causing fear or disquiet or impairing their freedom of judgement. | Semipublic |

| | | |
|---|---|---|
| Article 154 - A , paragraph 2 | The attempt is punishable. | |
| Article 192º - **Privacy intrusion** | To intercept, record, use, transmit or divulge a conversation, a telephone communication, email messages or detailed billing; to capture, photograph, film, record or divulge images of people or of objects or intimate spaces; to observe or listen, in hiding, persons who are in a private place or to divulge facts relating to the victim's private life or serious illness, without the victim's consent and with the intention of intruding in the victim's private life, in particular in their family or sexual intimacy. | Semipublic |
| Article 194 - **Breach of correspondence or telecommunications** | Open a parcel, a letter or any other writing that is closed and that is not addressed to oneself, or become aware, by technical processes, of its content, or prevent, in any way, that it is received by the recipient; interfering in the content of telecommunications or become aware of them and disclose the content of closed writings or telecommunications. | Semipublic |
| Article 199.º - **Illicit recordings and photographs** | To record, without consent, words spoken by another person and not intended for the public, even if addressed to them; to use or permit to use such recordings even if lawfully produced; to photograph or film another person, even at events in which they lawfully participated or to use or permit to use such photographs or films already mentioned, even if lawfully obtained. | Semipublic |
| Article 199.º, paragraph 2, b) | Disclosure of unauthorized images. | |
| Article 240.º, paragraph 1, al. a) and b) - **Discrimination and incitement to hatred and violence** | Establish or constitute an organisation or engage in organised propaganda activities that incite or encourage discrimination, hatred or violence against persons or groups of persons because of their race, colour, ethnic or national origin, ancestry, religion, sex, sexual orientation, gender identity or physical or mental disability; or participate in or provide assistance to the organisation or activities referred to in the preceding subparagraph, including funding. | Public |
| Article 240.º, paragraph 2, al) a | Through justification, denial or gross trivialisation of crimes of genocide, war or against peace and humanity, publicly, by any means intended to publicise, provoke acts of violence, defame or insult, threaten or incite to violence or hatred, against persons referred to in paragraph 1. | |
| Article 223.º - **Extortion** | To coerce another person, with the intention of obtaining for himself or for a third person unlawful enrichment, by means of violence or threat with a major evil a patrimonial disposition that causes damage for that person or for another person. | Public |
| Article 223.º, paragraph 2 | Where the threat is the disclosure, through the media, of facts which could seriously damage the reputation of the victim or another person. | |

The provision in **Article 152, paragraph 2, b) - Domestic Violence** was introduced by Law 44/2018. This new precept aims at protecting personal data (namely image or sound, which includes videos, films, photos) on intimacy (namely sexuality) in particular and the privacy of any victim when disseminated (posted/spread) through the Internet or other means of widespread public dissemination (such as through social media and networks), without the victim's consent. This criminalisation was aimed at further penalising, through this special qualification, cyberstalking within domestic violence (understood as a conduct consisting mainly, according to Carolina Villacampa Estiarte, of "sending offensive or threatening e-mails, text messages and instant messages, publishing offensive comments about the victim on the Internet, sharing intimate photographs or videos of the victim via the Internet", which are experienced as "more intrusive for the victims" and which "cause them more adverse psychological effects").

Regarding **article 176 - Pornography of minors**, the conducts listed go beyond those described in Directive 2011/93/EU, despite not being as advanced as the Lanzarote Convention. In this sense, one should note the recent Law 40/2020 of August 18 which amended some paragraphs of this article and also added the article 176-B regarding the organisation of trips for purposes of sex tourism with minors to the Portuguese Penal Code.

**Article 176-A - Enticing minors for sexual purposes** was added to the Penal Code by Law No. 103/2015, of August 24. Thus, complying with the provisions of Directive 2011/93/EU, new forms of sexual abuse and exploitation facilitated by the use of ICT, such as, for example, grooming of minors through the Internet, pornographic performances in real time on the Internet, or knowingly and intentionally accessing child pornography hosted on certain Internet sites, have become criminalised.

**Article 193 – Intrusion via means of ICT**, derives from the constitutional precept laid down in Article 35(3) of the Portuguese Constitution. It aims at protecting privacy against possible acts of discrimination made exponentially dangerous by the use of computerised means. This is why the criminal procedure concerning this crime does not depend on filling a criminal complaint. It is thus a public crime, on which the State will always have an interest and duty to act. The criminalised conducts of the crime of intrusion via means of ICT, include not only the act of creating files that violate the legal good (privacy), but also the mere act of keeping and using those files, even if without any co-participation in its creation. The definition of the crime is thus quite comprehensive regarding the penalised conduct and is intended to have a deterrent effect in view of the difficulty of proving who is the material author of the file. In the same sense, the mere attempt is penalised.

The criminalisation of **computer fraud and communications** laid down in **Article 221** is aligned with developments in the general area of fraud, sharing the same defining elements of the generic crime of fraud described in Article 217 of the Penal Code – the intention to obtain for oneself, or for a third party, illegal enrichment and causing patrimonial damage to a third party. Similar to the crime of fraud, with respect to the crime of computer fraud and communications the attempt is also punishable, and the criminal procedure depends on filling a criminal complaint. The **specificity of this crime** lies in the action's process: the **use of ICT means**, i.e. the use of computerised means in a cunning way to manipulate

data or results. Paragraph 1 of the Article refers to interference with the result of data processing aimed at obtaining an illegal advantage, while paragraph 2 refers to the use of ICT aimed at disrupting the integrity/normal functioning of computer systems to obtain an illegal advantage.

It is now necessary to analyse other offences that, although they do not expressly provide for the use of ICT means, have a high probability of using these means, given the exponential increase in access to the Internet and smartphones;

**Article 194 - Breach of correspondence or telecommunications**, the crime is aggravated if the contents are disseminated through the Internet (cf. art. 197 Penal Code). This article derives from the fundamental right provided for in Article 34 of the Portuguese Constitution, which enshrines the secrecy of communications, defining its breach as a crime. It is also applicable to electronic correspondence (via e-mail) and all other electronic communications and mobile telephone services (SMS, etc.) that are modernly comparable to sealed postal correspondence. The legal good protected in this provision are privacy, protection of freedom of expression and community trust in the integrity of the means of communication, namely telecommunications and security.

Protection is given to both the content of electronic communications and the circumstances of communication (traffic data). Simply keeping data is a breach, which repeats itself in each new use or utilisation of the content of the traffic data. In electronic communications, for the crime to be completed, it is not required to know the content, just the access suffices (as it is not necessary to 'open').

The question arises as to whether this crime is not absorbed by the crime of 'unlawful interception' set out in Article 7 of Law 109/91. It seems to us that, although there may be an overlap when the message is intercepted during its transmission, that will no longer be the case when the message is accessed after it has already been received by its recipient, and it is stored in its electronic mailbox. Although, in the latter case, it could also be said that this amounts to 'unlawful access' provided for by article 6 of the Cybercrime Law, we believe that this is not the case as this crime requires a **special intention: "intention to achieve, for yourself or for others, an illegal benefit or advantage"**, which the crime of 'breach of correspondence or telecommunications' does not require. It would not be reasonable, therefore, that a closed electronic mail, once received, would be less protected than paper mail. We therefore understand that this crime still applies to electronic mail.

Still under the scope of the protection of privacy or private life, we find the following crimes: **home invasion or the violation of privacy** (art. 190 Penal Code), **trespassing in a place closed to the public** (191 Penal Code), **breach of private life** (art. 192 Penal Code), **violation of secrecy** (art. 195 Penal Code). In all of them, an aggravation is foreseen if the contents are disseminated through the Internet, cf. art. 197 Penal Code).

The provision regarding **illicit recording and photographs** laid down in **art. 199 of the Penal Code** intends to safeguard the right to protect one's own image, which is an autonomous legal and penal good protected in itself and independently from the point of view of the privacy or intimacy portrayed.

The right to one's own image covers two autonomous rights: the right not to be photographed and the right not to have the photograph published. The person concerned may authorise or consent to being photographed and may not authorise the use or publication of that photograph. The subject cannot not be photographed, or their photograph used against their will.

Example: João, against Maria's will, uses her photo, which was lawfuly obtained - Maria consented on being photographed – and publishes it on *Facebook*.

In addition to these, other crimes can be committed and their effects enhanced by using technologies. **These are crimes whose typology does not consider the use of technology as a constitutive element of the crime**.

**Stalking**, defined in **art. 154-A Penal Code**, can be committed by electronic means: cyberstalking. It tends to occur over long periods of time, with consequences, in many cases, becoming more serious over time. Due to this, the crime of stalking can integrate other types of crime, e.g. art. 193 Penal Code, which defines intrusion by ICT means, recording crime, and illicit photographs provided for in art. 199 Penal Code.[49] Also, the crime of **discrimination and incitement to hatred and violence**, laid down in **article 240**, can be committed by electronic means.

The crime of extortion, provided for in Article 223 of the Penal Code, is normally associated with the practices of ransomware, especially with the blocking of a given system, by encrypting the data stored in it or its operative files, and requiring, in exchange for its unblocking, a large amount of money (normally to be paid in Bitcoins).

**Other examples:**

Crimes against honour committed by including insulting expressions or accusations in online pages, blogs or disseminating them by email. The electronic medium is relevant as it is used for the disclosure of the insulting or defamatory content and it has a greater potential for damaging the protected legal good (cf. Art. 183, nº. 1, a) Penal Code: offense practiced through means that facilitate its dissemination; and Art. 183, nº. 3 Penal Code: media of mass communication, e.g. social networks).

**Decree Law No. 7/2004 of January 7** transposed Directive 2000/31/EC. Thus, this instrument establishes the principle of exemption from liability of intermediary providers of network services in the face of possible illegality of the messages they make available. In this sense, one departs from the absence of a general duty of vigilance on the part of the intermediary service provider with regard to the information that it transmits or stores or to which it provides access (art. 12), to an obligation to inform/communicate immediately to the Public Prosecutor Service whenever they are aware that the provision of content through the services that they provide, or access to them, can constitute a crime (art. 13 a))[50] The most recent amendment introduced by Law 40/2020 August 18 extends this duty of information and reinforces it in relation to any case of detection of content made available by the service provider that may constitute a crime, namely the crime of pornography of minors or the crime of discrimination and incitement to hatred and violence.[51]

[49] V Cibercrime and Stalking, Vânia Costa Ramos, p. 11. https://carlospintodeabreu.com/public/files/cibercrime_stalking.pdf

[50] Not particularly relevant for the perspective of victim support, but relevant as an example of how ISP's intervention can occur, see the Memorandum of Understanding concluded between IGAC (General Inspection of Cultural Activities), ISP's and associations representing intellectual property owners, with a view to facilitating the identification and removal/blocking of pages disclosing content manifestly infringing copyright. Cf. http://www.apel.pt/gest_cnt_upload/editor/File/apel/direitos_autor/memorando_APRITEL_IGAG_MAPINET.pdf

[51] See new Article 19-A of Decree-Law No. 7/2004, added by Law 40/2020 August 18.

In addition to this duty to notify the authorities, Intermediary Service Providers have the obligation to block or remove content of a **manifestly** illegal nature (cf. art. 13 c); art. 15, para. 3; art. 16, para. 1; art. 17), in cases where they become aware of its existence - by themselves or through third parties. With the changes introduced by Law 40/2020 August 18, providers are obliged to remove, within 48 hours, contents pertaining to sexual abuse or exploitation of minors.[52]

Failure to comply with the specific duties of informing and blocking gives rise to the liability of the Intermediary Service Providers, either through the mechanism of Civil Liability (art. 16) or through the enforcement of Administrative Offences (art. 37) by the entity responsible for Supervision – ANACOM.

**Law 32/2008 of 17 July 2008**, known as the Data Retention Act (in Portuguese Lei da Retenção de Dados, LRD) in the context of the provision of electronic communications services for the investigation, detection and prosecution of serious crimes by the competent authorities. It transposed Directive 2006/24/EC, no longer in force in EU law.[53] However, that law is still in force in the Portuguese legal system. The most relevant provisions on the preservation of digital evidence can be found in article 4, paragraph 3, which defines what are serious crimes for the purposes of this law, thus presenting a catalogue of crimes whose investigation will allow the use of data retained by service providers and article 6, which provides for a **period of one year for storage of traffic and location data** in the electronic communications sector.

Finally, **Law 46/2018 of 13 August** establishes the **legal framework for cyberspace security** (in Portuguese, Regime Jurídico da Segurança do Ciberespaço), and transposes Directive (EU) 2016/1148 on measures to ensure a high common level of network and information security throughout the Union[54]. It created the Cyberspace Security Superior Council (in Portuguese Conselho Superior de Segurança do Ciberespaço, CSSC), as a specialised advisory body to the Prime Minister on matters relating to cyberspace security. In Articles 5 and 6 the law defines the competencies of the CSSC and in Article 7 it defines the competencies of the National Cybersecurity Centre (in Portuguese, Centro Nacional de Cibersegurança CNCS). In articles 8 and 9, the law provides the legal framework for the National Computer Security Incident Response Team – in Portuguese Equipa de Resposta a Incidentes de Segurança Informática Nacional CERT.PT - and defines its competencies, integrated in the CNSC. This law also establishes minimum cybersecurity requirements and incident reporting obligations at all government levels and public entities, critical infrastructure service providers, operators of essential services and digital service providers, before the CNCS, which subsequently informs, if necessary, the contact points of other affected Member States.

On June 12, 2019, the Government adopted the **Resolution of the Council of Ministers No. 92/2019 that approved the first National Strategy for Cyberspace Security**, aiming at improving the security of networks and information systems and enhance the free, safe and efficient use of cyberspace by all citizens and public and private entities. The strategy is based on three principles: subsidiarity of state intervention, complementarity of action (close liaison and co-ordenation with various actors) and proportionality (in the allocation of resources and services to face digital threats).

[52] See Article 19 B of Decree-Law No. 7/2004, added by Law 40/2020 August 18, which expressly requires the removal, within 48 hours, of content of sexual abuse or exploitation of minors.

[53] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX-:32006L0024&from=PT

[54] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of network and information security throughout the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=PT

### 2.3.2. The case of Romania

The Romanian legal system has no special law on cybercrime. In this sense, the legal provisions for this type of crime are laid down in the Romanian Penal Code under two different titles:

Title II - Crimes against property
Chapter IV - Fraud through computer systems or electronic means of payment:

- Computer fraud (Art. 249), defined as the conduct of "introducing, modifying or deleting computer data, restricting access to such data or, in any other way, preventing the normal operation of the computer system, with a view to obtaining a patrimonial advantage from which damage may result";
- Carrying out fraudulent financial transactions (Art. 250) - "carrying out operations of cash withdrawal, deposit or downloading of electronic payment instruments or transfer of funds through the use of electronic means of payment without the consent of the owner or data enabling their identification";
- Acceptance of fraudulent financial transactions (Art. 251) - "acceptance of the above transactions in full knowledge of their fraudulent nature";

Title VII - Crimes against public security
Chapter VI - Crimes against the security and integrity of computer systems and data

- Unlawful access to a computer system (Art. 360), which differentiates between unlawful access to a computer system, unlawful access to a computer system for the purpose of obtaining computer data, and unlawful access to a computer system that has programs, devices or procedures that restrict access to it. The three types of crime corresponde to increasingly severe penalties;
- Unlawful interception of electronically processed data (Art. 361)
- Modification of the integrity of computer data (Art. 362) - "unlawfully modify, delete, deteriorate or damage computer data or restrict access to them";
- Disruption of the operation of computer systems (Art. 363) - "serious and unauthorised disruption of the operation of computer systems in the form of the input, transmission, modification, erasure or deterioration of computer data or the restriction of access to them";
- Unauthorised transfer of computer data (Art. 364)
- Illegal operations in computer devices or software (Art. 365) - "produce, import, distribute, supply or unlawfully possess devices, programs, passwords and access codes that allow total or partial access to the computer system for the purpose of committing the crimes foreseen in Articles 360 to 364.

Title VIII - Crimes affecting social coexistence relations
Chapter I - Crimes against peace and public order

- Child pornography (Art. 374), defined as the conduct of "producing, possessing, obtaining, preserving, exposing, promoting, disseminating or divulging, and/or in any way providing pornographic

content featuring minors, as well as extorting or recruiting minors for the purpose of participating in a pornographic show, thereby obtaining an advantage, or otherwise exploiting minors for the purpose of performing a pornographic show". The viewing of pornographic content concerning minors is also punishable by law. The cybercrime component in child pornography is evident in Article 374, paragraph 2, in the part where it expressly mentions the sanctions for the conducts mentioned above, whether committed by means of a computer system or any other electronic communication means. In addition, paragraph 4 expressly includes new information and communication technologies as means of communication for pornographic performances.

Attempting to commit any of the above conducts is punishable in accordance with Articles 252, 366 and 374(5) of the Romanian Penal Code.

The country's commitment to combating cybercrime was reinforced in 2011 when the government created the National Computer Security Incident Response Team (in Romanian: *Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică* - CERT-RO), which consists of an independent and specialized centre for research and development in cybersecurity. In 2013, Romania approved the National Strategy for Cybersecurity, which also aimed at creating a National System for Cybersecurity (in Romanian: *Sistemul naţional de securitate cibernetică* - SNSC), which is based on a general framework for cross--sector cooperation between public authorities and industry institutions or representatives.

In July 2020, Law 217/ 2003 on the prevention and combating of domestic violence was amended and cyber violence was included among the recognised forms of domestic violence, alongside verbal, physical, sexual, psychological, economic, spiritual and social violence. According to Law 217/ 2003, cyber violence is defined as "online harassment, online hate speech, online stalking, online threats, non-consensual publication of information and intimate graphic content, illegal access to interception of private communications and data, and any other form of misuse of information and communication technologies via computers, smartphones or other similar devices that use telecommunications or connect to the Internet and can transmit and use social or email platforms with the aim of tormenting/shaming, humiliating, intimidating, threatening or silencing the victim".[55] It is important to note that these provisions refer to intentional actions or inactions that include any of the above-mentioned forms of violence and that occur "in a domestic or family environment, between spouses or ex-spouses, between partners or ex-partners, regardless of whether the aggressor resides or has resided with the victim" (Art. 3).

Finally, at the time this Handbook was concluded, a proposal to sanction non-consensual pornography (or so-called 'revenge pornography'[56]), adopted by the Senate on 21 October 2019, and subsequently sent to the Chamber of Deputies for debate, is under consideration in the Romanian Parliament. The proposal seeks to amend Article 226 of the Penal Code (which regulates the offence of violation of privacy) to include the offence of non-consensual pornography, defining for this purpose the conduct of "sharing, presenting or transmitting intimate images, by whatever means, of a person without their consent", the practice of which could carry a prison sentence of between 3 months and 2 years or a fine.[57]

[55] Article 4 (h) of Law 217/ 2003, as amended by Law 106 of 3 July 2020.

[56] The author advises against the use of the term 'revenge pornography' as this implies that the victim is at fault and the perpetrator is disclosing the material as a form of punishment. Furthermore, 'pornography' implies material produced for a wider public and/or for sexual arousal, while in many of these crimes the aim is primarily to control and abuse the victims. Therefore, the preferred terminology is 'non-consensual distribution of sexual material'.

[57] For more information on the proposed law on non-consensual pornography, see https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019.

### 2.3.3. The case of Germany

With the entry into force of the Lanzarote Convention and the Budapest Convention, German criminal legislation was adapted to incorporate the recent developments in the field of Internet and computer-related crime. Subsequently, German legislation also incorporated important EU directives on cyber attacks and protection of children against sexual abuse and exploitation of minors and child pornography. Important changes were the criminal definition of grooming of minors and the amendment of the penalties according to the Lanzarote Convention.

The **BKA** (Criminal Department of the Federal Police) is the **public authority** responsible for **cybercrime**, internally and in terms of international cooperation, especially in the area of online card fraud. The BKA also works directly in the fight against cyber crime with agencies such as Interpol and Europol.

The Ministry of the Interior has been developing national strategies to combat cybercrime, strengthen security in telecommunications and computer systems and improve the protection afforded to Internet users in Germany.[58] The first strategy came into force in 2011 and its objectives are still largely applicable today. However, the rapid evolution of the phenomenon has made it necessary, in 2016, to complement these objectives and to group them in a new strategy that is transversal to services in order to promote and speed up cooperation between different stakeholders, taking into account the cross-sectoral nature of cybercrime.[59]

Regarding the legal diplomas concerning the fight against cybercrime, starting from the constitutional precept which foresees the inviolability of telecommunications, through to the provisions on crime in the German Criminal Code and ending in separate legislation such as the **Telecommunications Act (**Telekommunikationsgesetz **TKG**), the **Telemedia Act (**Telemediengesetz **TMG)**, the **Computer Security Act (IT-Sicherheitsgesetz)** and the **Facebook Act (**Netzwerkdurchsetzungsgesetz **NetzDG)**, the German legal system appears to be legally well equipped to combat the dynamic and cross-border reality of cybercrime, investing in strong national cooperation with private industry entities.

The same applies to the **Youth Protection Act (JuSchG)** which aims at strengthening and protecting children and young people by restricting access to health-endangering products, to cinematic films and media on image carriers and to stays in certain places in the public domain to certain age groups. There is a discussion going on at present for the Act to be amended with the main focus on preventing cybergrooming and cybermobbing.

**Article 10 of the German Constitution** protects the inviolability of the secrecy of postal and telecommunications correspondence.

As far as criminal law is concerned, the **German Criminal Code (**Strafgesetzbuch **StGB)** brings together the main offences relating to cybercrime and there is no fragmentation between general criminal law and cybercrime law, unlike the Portuguese legal system.

[58] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany

[59] https://www.bmi.bund.de/cybersicherheitsstrategie/

The **StGB** foresees three types of criminal offences related to cybercrime:

1. Conducts concerning the **unlawful use of computer systems or data**, particularly related to cyber-attacks:

**Table I-5: Conducts concerning the unlawful use of computer systems or data**

| Article and heading | Conduct | Article in CCCE |
|---|---|---|
| § 202a – **Data Espionage** | Obtaining unauthorized access to electronically transmitted data (or an information system) not intended for those accessing it or unauthorized access to specially protected data, bypassing security mechanisms (e.g. encryption). | 2 |
| § 202b – **Interception of computer data (Phishing)** | Obtain data to which access is not authorized using a non-public data transmission or electromagnetic radiation from a data processing system to oneself or to another person for whom the communication is not intended.<br><br>Allows for *concursus* with other crimes. | 3 |
| § 202c – **Acts preparatory to espionage and unlawful interception of computer data (phishing)** | Practice of preparatory acts for the infractions foreseen in § 202a and 202b; e.g. produce, obtain for oneself or others, sell, supply, disclose or make public, security codes that allow access or computer programs whose purpose is the practice of such acts. | 6 |
| § 202d – **Unlawful handling of computer data** | Obtain, supply, deliver, distribute or make available data that is not generally accessible or open to the public, and that has been **obtained by another person through an illicit act**, in order to enrich oneself or others or to harm another person. Exception: acts carried out exclusively in compliance with legal obligations, e.g. public authority in the context of an investigation. | |
| § 303a – **Computer Data Manipulation** | Delete, supress, render unusable or modify computer data. | 4 |
| § 303b – **Computer sabotage** | (1) Significantly interrupt a data processing operation that is of essential importance to another person by performing the acts described in § 303; or by entering or transmitting data with the intent to inflict another disadvantage; or by destroying, damaging, rendering unusable, removing or altering a data processing system or data carrier.<br><br>(5) Applies to § 202c, concerning the condemnation of preparatory or facilitating acts. | 5 |
| § 269 – **Forgery of computer data** | In order to mislead legal relations, to store or alter relevant evidence in such a way that a false or falsified document is produced, or to use data stored or altered in this way. | 7 |
| § 270 – **Falsehood in processing of data** | Deception in legal relations is equivalent to interference in computerised data processing in legal relations. | 7 |

2. Conducts corresponding to an **action whose practice requires the use of electronic means as a tool** for committing the crime:

**Table I-6: Conducts corresponding to an action whose practice requires the use of electronic means as a tool**

| Article and heading | Conduct | Article in CCCE |
|---|---|---|
| § 206 – **Violation of secrecy of post or telecommunications** | [1] communicate to another person, without authorisation, facts which are subject to postal or telecommunications secrecy and of which one has become aware as owner or employee of a company providing postal or telecommunications services on a commercial basis.<br><br>[5] The secrecy of postal traffic extends to the detailed circumstances of the delivery and its contents. The **content of telecommunications and its specific circumstances** [for those involved in a telecommunications operation], **are subject to the secrecy of telecommunications**. Telecommunications secrecy also extends to the circumstances of **unsuccessful connection attempts**. | |
| § 263a – **Computer fraud** | [1] With the intention of obtaining an unlawful patrimonial advantage for themselves or for a third party, to damage the property of another person by influencing the result of a data processing operation through the incorrect design of the program, the use of incorrect or incomplete data, the unauthorized use of data or any other unauthorized influence on the operation.<br><br>[3] Preparatory acts such as production, acquisition, offer for sale, maintenance in security or delivery to another person of computer programs whose purpose is the practice of such crime. | 8 |
| § 265a – **Obtaining services by deception** | Use a **telecommunication**s machine or **network** which serves public purposes, in order not to pay the fee due for a means of transportion, or access to an event or facility. | |

3. Conducts corresponding to an **action that can be practiced** - but not necessarily - **through the use of electronic means** as a tool for committing the crime.

In this case, it is important to note that **§ 11(3)** provides that media such as **sound and image media, data storage media**, illustrations and other representations are to be treated in the same way[60] for the purposes of the articles referring to this paragraph. It follows that the following offences involved conducts by electronic means:

[60] This provision is currently under review and will be adapted to the new challenges of cybercrime. In the Government Bill of 4 September 2019, section 11(3) reads: "The contents within the meaning of the provisions under this paragraph are those contained in writing, on sound or image media, on data storage media, illustrations or other representations or **are transmitted independently of storage via information or communication technology**". The bill has not yet been approved.

**Table I-7:**

| Article and heading | Conduct |
|---|---|
| § 86 – **Dissemination of propaganda material of unconstitutional organizations** | lUse propaganda materials - referred to in 11 [3] - which, according to their content, are directed against the free democratic basic order or to the principles of international law, are distributed in Germany or are produced, stored, imported or exported for distribution in Germany or abroad, or made accessible to the public on data storage devices. |
| § 88 – **Anti-constitutional sabotage** | [1] whoever acts with the intention of interfering ...<br><br>[2] public service telecommunications facilities. |
| § 91 – **Incitement to committing serious violent offences against the State** | Displaying or providing to another material referred to in 11 [3] which, by its contents, is capable of serving as an instruction to commit serious and violent offences against the State [§ 89a], if the circumstances of its dissemination are conducive to incitement or encouragement of others to commit such offences, and/or<br><br>[2] Obtain materials 11 [3] for the purpose described in [1] of this article. |
| § 130 – **Incitement to hatred** | [2] Incite hatred, call for violent measures or attack the human dignity of a group or sections of the population or an individual because of their membership of a group, by the means referred to in 11 [3], by disseminating materials to the public through telecommunications.<br><br>[5] Publicly approving, denying or downplaying an act of hatred committed during the rule of National Socialism and disturbing the public peace in a manner that violates the dignity of the victims by approving, glorifying or justifying the conduct of the National Socialist regime of violence and arbitrariness, is equally punishable if telecommunications are used for its commission. |
| § 131 – **Depictions of violence** | [1] By the means referred to in 11 [3], describe acts of cruel or inhuman violence against human beings or glorify or trivialize such acts through dissemination to the public or through production, acquisition, supply, keeping stock, offer, advertising or undertaking to importing or exporting such content, by using means of radio broadcasting and telecommunications. |
| § 201a – **Violation of intimate privacy by taking photos or other images** | [1] Creation or transmission/dissemination of unauthorized image recording of another person in their private, intimate sphere.<br><br>[3] Taking photographs, producing or supplying to a third party in exchange for benefit or, obtaining for themselves or a third party, material relating to the nakedness of persons under 18 years of age. |
| § 238 – **Stalking** | Severely disrupt another person's life in such a way as to seriously affect their lifestyle by persistently: 1. seeking physical proximity to that person, 2. trying to establish contact with that person through the use of telecommunications, 3. Improperly using that person's personal data for the purpose of [a] ordering goods and services on that person's behalf, [b] inducing third parties to make contact with that person, or 4. threatening that person, or one of their relatives, or someone close to them, with injury to life, physical integrity, health or liberty. |

With regard to crimes related to minors, although falling into the latter category (3), they are treated here separately:

**Table I-8:**

| Article and heading | Conduct | Article in CCCE |
|---|---|---|
| § 176 – **Child sexual abuse** | [1] Performing sexual acts with children under 14 years;<br><br>[2] Inducing or influencing a child to perform acts of a sexual nature;<br><br>[4] Engaging in sexual activities in the presence of a child or presenting pornographic content to the child through the means described in § 11[3] or through **information and communication technologies** in order to induce the child to engage in sexual activities with the offender or a third person, or in their presence, or to influence the child to engage in acts for the production of child pornography content;<br><br>[5] Offer or promise to supply content with children relating to the acts described from [1] to [4]. | 9 |
| § 176a – **Aggravated sexual abuse of minors** | [3] Performing the acts described in § 176 as the principal offender or otherwise involved in the commission of the acts, with the intention of making the act the object of pornographic content [§ 11 [3]] to be disseminated as described in § 184b. | |
| § 184b – **Dissemination and procurement of child pornography (under 14 years)** | Disseminate, display or otherwise make available to the public, sexual content of minors, or produce, obtain, supply, stock, offer, recommend, import or export for those purposes, or otherwise facilitate/support the use of the means described in § 11[3] relating to sexual content of minors (includes sexual acts performed with minors, acts performed in the presence of minors or the reproduction of a child full or partially undress in an explicit sexual pose or the reproduction of a child's genitalia or buttocks).<br><br>[5] Excludes application in cases of legal pursuit of public functions (e.g. in criminal proceedings). | |
| § 184c – **Dissemination, procurement and possession of youth pornographic literature** | By the means described in § 11 [3], disseminate or make available to the public, undertake to deliver to another person, or to produce, obtain, supply, stock, offer, advertise or import or export a type of youth pornography [between 14 - 18 years]. | |
| § 184d – **Dissemination of pornographic content via radio broadcasting or telecommunications** | [1] Making pornographic content available to another person or to the public **via radio or telecommunications** is punishable under the provisions of §§ 184 to 184c [Does not apply to cases described in § 184[1] - dissemination of pornographic content - provided that such content relates to persons over 18 years of age and is not accessible to persons under 18];<br><br>[2] This also applies to §§ 184b [3] and 184c [3]: anyone who undertakes to procure child pornography content by electronic means shall also be punished. | |

The attempt is punishable under sections 263a(2) in conjunction with § 263(2), § 269(2), § 263a(3), § 303a, § 303b (vg. § 303a(2) and 303b(3)). For crimes related to child abuse, the attempt is also punishable; § 176(6). Exception: § 176(4)3 and 4 and § 176(5). Preparatory acts are punishable in crimes: § 202c, § 202a, § 202b, § 303a(1)(2) and § 303b (1)(5). Aiding and abetting is also punishable under § 26 and § 27 of the StGB.

Legal persons are not subject to criminal liability but may be held liable pursuant to §§ 30, 130 *Ordnungswidrigkeitengesetz* (OWiG), which concerns the Administrative Offences Act. Their legal representatives can be held liable pursuant to § 14 of the StGB.

It can thus be concluded that cybercrime *lato sensu*, where the Internet is used to commit the crime, extends to almost all offences.

The following list is not exhaustive but mentions other proeminent offences in Germany that can be committed through the use of the internet;

- § 253 of the Criminal Code, blackmail;
- Copyright infringements under the German Copyright Act;
- § 284 of the Criminal Code, unauthorised organisation of a game of chance;
- Drug trafficking under the German Federal Narcotics Act;
- Arms trade under the German Weapons Act;
- White-collar crime.

In addition to the criminal offences described above, German law also provides for other offences and misdemeanours in connection with acts relating to electronic communications and data protection, which we describe briefly.

The **Telecommunications Act (TKG)**, passed on 06.22.2004, provides a set of obligations for telecommunications service providers as private entities to observe in the pursuit of their activity. This law is also of particular importance in relation to the issue of preservation of digital evidence, as it forsees the obligation to report acts that may constitute breaches of the integratity of telecommunications and the obligation to retain certain data for criminal prosecution purposes in the event of particularly serious crimes.

Thus, **§ 88 Privacy of telecommunications** and **§ 89 Prohibition to intercept, obligation on receiving equipment operators to maintain privacy** protect the integrity and confidentiality of telecommunications and cover their content and detailed circumstances, e.g. who is or has been involved in a telecommunications process, and also extends to details of unsuccessful attempts to establish a connection. It is forbidden for the parties to obtain knowledge of these telecommunications beyond what is strictly indispensable for the exercise of their activity and the use of this knowledge for other purposes is permissible only to the extent allowed by law or other legal provisions. In this case, it is important to note that the duty to report provided in § 138 of the Criminal Code - obligation to report crimes of which they have knowledge - has priority in relation to the secrecy of communications.

**§90** prohibits the **misuse of transmitting equipment** by prohibiting the possession, manufacture, distribution, import or the introduction of any transmitter or other telecommunications equipment that is particularly apt and intended to hear the unspoken word of another person or to record the image of another person without that person noticing it.

**§96 and § 98** concern the conditions under which service providers may collect **traffic and location data** respectively. Therefore, only data indispensable for the purposes of their activity can be retained, and such data can be used only to the extent necessary and for the purposes mentioned in this Act or in compliance with other legal provisions. Otherwise, they must be deleted without undue delay.

**§109** obliges service providers to adopt **technical safeguards** to protect the secrecy of telecommunications, and against the violation of personal data protection, taking appropriate technical precautions in data processing in order to protect users against disruption caused by external attacks. Thus, measures should be taken to protect telecommunications and data processing systems from unauthorised access and to minimise the effects of security breaches on users or interconnected networks. Item (5) in this section also provides for a duty to report to the Federal Network Agency and the Federal Office for Information Security any deficiencies in telecommunications networks and services that could lead to significant security breaches. Similarly, **§ 109a** on **data and information security** establishes reporting obligations in case of a personal data breach to the Federal Network Agency and the Federal Commissioner for Data Protection and Freedom of Information of the breach and to the targeted users.

As to the retention of data for digital evidence purposes, **§ 113b** establishes the **obligation to retain traffic data** for 10 weeks for traffic data and for 4 weeks for location data. The content is excluded. The service provider erases the stored data irreversibly without delay, at the latest within one week after the end of the foreseen storage periods or ensures irreversible erasure, e.g. Right to be forgotten.

**§ 113c** lays down the **conditions under which stored data may be used** on the basis of **§ 113b**; they can only be transmitted to a prosecuting authority if the latter requires such transmission, refers to a legal provision allowing it to collect such data, and if the data relates to the prosecution of particularly serious criminal offences.

As a security measure, **§ 113d obliges providers to ensure the security of stored data** on the basis of the obligation under § 113b (1). Data must therefore be protected against unauthorised access and use by technical and organisational measures in line with the state of the art, through the use of encryption methods, among others.

The Federal Network Agency has the power to **monitor the enforcement of the obligations** laid down in this Act for service providers **(§ 115)**. The latter, in turn, are obliged to provide the necessary information to the Agency, which has the power to impose periodic penalty payments.

**The Telemedia Act (**Telemediengesetz **TMG)**, adopted on 02.26.2007, is applicable to all electronic information and communication services, unless they are telecommunications services. Note the obligation on providers of information services and web page or application services or for smartphones to ensure, by means of appropriate and economically proportionate agreements, that unauthorised access is not possible **(§ 13(7))**. On the other hand, there is also a **duty to provide information in case of unlawful access to data (§ 15a)**.

**The IT Security Act (*IT-Sicherheitsgesetz*)**, passed on July 25, 2015, gives jurisdiction to the federal prosecutors' office to investigate and prosecute crimes under 202a, 202b, 202c, 263a, 303a and 303b of the Penal Code.

It aims to strengthen computer and IT systems' security and is part of the cyber security strategy approved in 2011. To this end, it sets out obligations regarding a minimum level of computer security for telecommunications companies, digital service providers and critical infrastructure operators, e.g. it requires the implementation of an IT security management system, stipulates reporting obligations to the Federal Department of Computer Security (BSI) and to consumers in the event of a IT system breach, and requires the collection of information necessary to assess risks in the security of information technology, in the form of reports on attacks that have occurred, procedures adopted and imminent risks, to be reported to federal authorities (§ 4).

A proposal to amend this law, IT Security Act (IT-Sicherheitsgesetz) 2.0, was pending at the time of writing.[61] The new proposal is based on a change of strategy in the fight against cybercrime, which should no longer be defensive but offensive, through the use of different IT tactics.[62] The proposal also provides for increased penalties under the Criminal Code for cybercrimes under Sections 202a, 202b, 202c, 202d, 303a and 303b StGB. In addition, §§ 202e and 202f are inserted after § 202d StGB:

- § 200e - Unauthorised use of information technology systems;
- § 202f - Particularly serious offence against the secrecy and integrity of the ICT systems.

The ***Netzwerkdurchsetzungsgesetz* (NetzDG)**, published on 01.09.2017, commonly known as the Facebook Act, sets out obligations and establishes fines for social network providers in relation to the handling of user complaints about hate crimes and other illegal content on the Internet, as well as a quarterly reporting obligation on providers. It also confers the right to compensation for breaches of personal rights and the right to information on the data of the offender registered on that platform, before a court order.[63]

**§**1 (3) defines content that is considered illegal,[64] including discrimination and incitement to hate speech and extreme-right speech. §2 defines an obligation to report periodically on the handling of complaints about illegal content on their platforms. This report must be public. The Federal Office of Justice (BfJ) is the administrative authority that monitors reports, cf. § 4 (4).

**§** 3(2) 2 provides for the **obligation to remove or block access to manifestly unlawful content within 24 hours** of receiving the complaint, unless otherwise agreed with police or judicial authorities. Other illegal content must be removed, or access blocked without delay, within a maximum of seven days from receipt of the complaint, cf. § 3 (2) 3. In the event of removal, the provider is obliged to preserve the content for evidence purposes. Therefore, it stores such content for a period of ten weeks within the scope of Directives 2000/31/EC and 2010/13/EU, cf. § 3 (3).[65]

[61] https://www.whitecase.com/publications/article/germanys-draft-bill-it-security-20-extended-bsi-authorities-stricter-penalties

[62] https://netzpolitik.org/2019/it-sicherheitsgesetz-2-0-wir-veroeffentlichen-den-entwurf-der-das-bsi-zur-hackerbehoerde-machen-soll/#2019-03-27_BMI_Referentenentwurf_IT-Sicherheitsgesetz-2 and https://netzpolitik.org/2015/geheime-kommunikation-bsi-programmierte-und-arbeitete-aktiv-am-staatstrojaner-streitet-aber-zusammenarbeit-ab/

[63] Social network service providers with fewer than two million registered users in Germany are outside the scope of this Regulation.

[64] These are Articles 86, 86a, 89a, 91, 100a, 111, 126, 129, 129a 129b, 130, 131, 140, 166, 184b, in conjunction with Articles 184d , 185 to 187, 201a, 241 or 269 of the Penal Code.

[65] The NetzDG is currently under review and will be amended. The German Parliament and Council have already passed it, but the law has not yet entered into force. The new law will include an obligation for media operators to transmit the relevant data to the police forces.The aims are to strengthen users' rights, make information channels more user-friendly, simplify the execution of information requests and increase the information value of transparency reports.

Failure to comply with these duties shall result in administrative penalties.

Regarding procedural obligations, the special obligations provided for in Articles 16 and 17 of the Convention on Cybercrime are not specifically provided for in the **German Code of Criminal Procedure (StPO)**. However, the seizure of computer data, including requests for disclosure of data, is carried out under § 94 and § 98 StPO, which regulate the general seizure of tangible assets.

Article 18 of the Convention on Cybercrime is not provided as such in the StPO. In this sense, the request by the authorities of disclosure/information regarding computer data is covered by the provisions of § 95 StPO, concerning the duty to hand over relevant tangible assets for evidence in criminal proceedings.

The collection of real-time communication traffic data, provided for in Art. 20 of the Convention on Cybercrime, is subject to the requirements of § 100g StPO. This article also states which particularly serious crimes justify the provision of data by service providers (cf. § 113b TKG). **§** 100g (2) also provides for the possibility for the court to order the supply of traffic data and information to service providers in case of well-founded suspicions of the particularly serious crime listed in that article.

The interception of telecommunications or real-time data collection provided for in Art. 21 of the Convention on Cybercrime is regulated by § 100a and 100b. It must be subject to judicial authorisation at the request of the prosecutor. In general, the collection of data through online search and spyware is not admitted in the scope of criminal prosecution, except in the cases described in 100b.

§ 110 (3) - Possibility of access and inspection of storage media spatially separated from the main one that was under inspection, insofar as they can be accessed from the storage media. Example: external disks.

Requests for information and/or delivery of data from service providers to the authorities are regulated generally in § 100j StPO and particularly in separate laws; e.g. § 113 TKG.

The information and data shall be provided within the limits provided for in § 96(1), § 113a and 113b TKG (Telecommunications Act).

As far as **international co-operation** is concerned, Germany is involved in several European and international projects of bilateral co-operation in the area of cyber security:

- European Network and Information Security Agency (ENISA);
- The European Commission's AGIS programme, designed to help legal practitioners as well as judicial authorities and representatives of victim support services from Member States and other countries who apply, with a view to setting up a European network to exchange information and good practices;
- Interpol European Working Party on IT Crime (EWPITC), a platform for information exchange and combating IT crime.

The International Assistance Law, in German **Internationale Rechtshilfe in Strafsachen (IRG)** provides procedures and conditions for international assistance. Thus, Articles 29-31 of the Convention on Cybercrime concerning mutual assistance between countries are covered in this law.

Concerning cooperation with the Europol Cybercrime Centre, Germany is part of the Joint Cybercrime Action Taskforce (J-CAT).[66]

The 24/7 contact point in accordance with Article 35 of the Budapest Convention is established at the BKA in Wiesbaden together with the Interpol and G-8 contact point.

Furthermore, there are some **public-private partnerships** within Germany to **combat cybercrime, in particular**;

- Alliance for Cyber Security: promotes the sharing of information and experiences among the key players in the German cyber security arena and aims to act as an information platform about the prevailing risks in cyberspace and to promote knowledge sharing. A joint initiative of the German Federal Office for Information Security (BSI) and the German Federal Association for Information Technology (Bitkom);
- CERT Network - The CERT network is the alliance of IT emergency incident response teams.[67]

**Final notes:**

- Mere possession of malware is not incriminating. National legislation only incriminates these facts when a person uses them in a criminal manner.
- According to some professionals, legal provisions need to be introduced into the Criminal Procedure Code to allow for the use of data access tools such as hacking, bearing in mind that the security forces consider that they are one step behind offenders.
- In general, German law appears to be in line with European legal texts.
- However, there is no express transposition of Articles 4 and 5 of Directive 2019/713/EU, as two more general criminal offences (§§ 263a and 269 of the Criminal Code, respectively computer fraud and computer falsehood) must be used to cover offences related to the fraudulent use of non-cash payment instruments. § 152b of the Penal Code provides for the offence of falsifying payment cards, but makes no reference to the use of electronic means or through IT systems.

[66] https://www.europol.europa.eu/content/expert-international-cyber-crime-taskforce-launched-tackle-online-crime Participants: Austria, Canada, Germany, France, Italy, the Netherlands, Spain, UK and USA. Australia and Colombia have committed to the initiative.

[67] https://www.cert-verbund.de/

# 3. CRIMINOLOGICAL AND VICTIMOLOGICAL PERSPECTIVES FOR THE UNDERSTANDING OF CYBERCRIME

## 3.1. Criminological theories applied to cybercrime

In this chapter of the Handbook, we will briefly address different theories of crime and their application to cybercrime, with the aim of achieving a reading as comprehensive as possible of the phenomena of cybercrime.

The basis for such analysis is the premise that existing knowledge about *traditional crime* is also applicable to cybercrime, assuming therefore that *traditional crime* and cybercrime are not substantially different. In that sense, the criminological theories associated with *traditional crime* become valuable tools to explain cybercrime as well (Wall, 2005, Yar, 2005b *cit in* Bossler & Burruss, 2012).

However, it is important to stress that it is not possible to fully understand the criminal phenomena, and cybercrime specifically, through the exclusive lens of a single criminological theory or approach, and thus it is very important, even considering the complexity of the phenomena under analysis, to consider the intertwining of these (and other) perspectives in the search for a more robust understanding of cybercrime and cyber-victimisation (Yar & Steinmetz, 2019).

### 3.1.1. Individual perspectives

This approach suggests that individuals with low self-control are more likely to engage in illicit acts (Gottredson & Hirschi, 1990 *cit in* Maimon & Louderback, 2019).

In this regard, Gottfredson and Hirschi (1990 *cit in* Higgins, Ricketts & Wolfe, 2014) argued that people with **low self-control** are less able to resist temptation when faced with an illicit opportunity, minimising the consequences of their actions, due to the characteristics associated with this individual trait, namely impulsiveness and insensitivity (Gottfredson & Hirschi, 1990 *cit in idem*). In this sense, crime is attractive, since it provides immediate benefits, without considering or anticipating long-term impacts, both at the individual level and for others.

Applying this explanatory approach of *traditional* crime to the understanding of cybercrime, the association between the *individual characteristics of the cybercrime* perpetrator and *cybercrime* does not seem to be linear, as research does not show unanimously that low levels of self-control represent (or not) an individual risk factor for the practice of cybercrime (Maimon & Louderback, 2019).

In the case of cybercrime, individual characteristics may not be so significant, since cybercrime involves a minimal (or even non-existent) direct interaction between victim and offender. For example, in the case of malware, it is difficult to determine who the actual victim of the infection by the malicious software will be, since any computer can potentially be infected, regardless of the individual characteristics of the players (Ngo & Paternoster, 2011).

On the other hand, the levels of self-control seem to impact on the risk of victimisation. Schreck, Stewart and Fisher (2006 *cit in* McNeeley, 2015) identified an association between low self-control and lower propensity to avoid risk behavior (such as involvement in delinquent activities and socialisation with deviant peers), even after personal experiences of victimisation. This link between low self-control and repeated victimisation was confirmed by Turanovic and Pratt (2014 *cit in* McNeeley, 2015): people with low self-control levels were less likely to make changes in their lifestyles, even after victimisation experiences.

HIGHLIGHT | INFORMATION IN FOCUS:

Some cybercrime studies, especially on cyber-dependent crime, have identified **individual risk factors associated with perpetration**:

- There are studies stating that, in the case of cyber-dependent crimes, most perpetrators have **relatively low technical capability** (NCA, 2016 *cit in* Maimon & Louderback, 2019).
- Others indicate, the association of cyber crime with **psychological and cognitive characteristics**, such as curiosity, creative thinking, problem-solving capacity, systematic and technical thinking (Rogers, 2006, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019).

Other authors (Morris, 2011 *cit in* Maimon & Louderback, 2019) point to the fact that the cybercrime perpetrator, particularly in the case of cyber-dependant crimes, develop **clearly external causal attributions**, such as techniques of neutralisation and rationalisation, denying the existence of the victim, cybercrime and/or responsibility in the act and/or blaming the victim for the fact that the practice of cybercrime was possible.

In the case of hacking, van der Hulst and Snow (*cit in* Koops, 2010) distinguished between 3 types of hackers, associated with different motivations:

- young male criminals whose cybercrime practice is associated with fun, curiosity or respect for peers;
- ideological hackers, who are intelligent and eager to learn, some of whom are obsessive and antisocial;
- financially motivated hackers.

### 3.1.2. Cybercrime as a rational choice

With an approach opposite to the previous one, within neo-classical criminology, crime emerges as the result of rational cognitive processes of reflection and decision by the respective perpetrators. This means that crime corresponds to a **rational decision on the part of its agent**, who analyses the costs and benefits associated to its practice, and whose choices/decisions are guided by those same processes of analysis and reflection (Cornish & Clarke, 1986 *cit in* Yar & Steinmetz, 2019).

Following this approach, if the potential offender perceives the costs associated with committing a crime, which may include the probability/risk of being caught and the associated legal consequences, as low, compared to the gains or benefits eventually obtained in the event of such a crime being committed, the probability of the crime occurring increases (Nagin, 1998 *cit in idem*).

Based on this interpretation, the increase in **perceived costs associated with committing a crime** and/or the reduction in the perception of the **benefits, gains and/or rewards from committing it** may contribute to the mitigation of crime (Cornish & Clarke, 1986 *cit in idem*).

Studies such as Louderback & Antonaccio (2017) point to the fact that reflective cognitive processes can reduce or increase the risk of involvement in cybercrime. This rationale is based precisely on the fact that **cybercrime is understood as a choice**, in which a rational evaluation of the efforts, costs and rewards associated with a certain behaviour is carried out (Cornish, 1993 *cit in* Maia et al., 2016).

Some studies associated with the application of this approach in explaining cybercrime (e.g. Bachmann, 2008, Hutchings, 2013 *cit in* Yar & Steinmetz, 2019) point to the fact that the cybercrime perpetrator effectively makes rational choices in the selection of their targets and also in the adoption of risk behaviors.

The rational choice also seems to take place even when targets show clear indications of being able to trigger consequences associated with the practice of cybercrime, which are there as deterrants. This leads to a modification of the criminal behaviour but not necessarily to its deterrence (e.g. Maimon et al., 2013 *cit in idem*).

### 3.1.3. Lifestyle Theory

The **lifestyle exposure theory** developed by Hindelang, Gottfredson and Garofalo (1978 *cit in* Phillips, 2015) states that a person's daily lifestyle influences the amount of exposure to places and times where there is a higher risk of crime.

In this sense, differences in victimisation rates across different demographic groups are precisely due to variations in lifestyle, which include routine daily activities, vocational activities (including professional and school/academic occupations), and leisure activities (Hindelang et al., 1978, p. 241 *cit in* McNeeley, 2015), and which may increase or decrease exposure to high-risk places and people at times when crime is most likely to occur.

The same theory postulates that demographic characteristics, such as age, gender, marital status, socioeconomic status, education and occupation, affect lifestyles, since they result in implications for the socially constructed roles, behaviours, activities and attributes that a given society considers appropriate for a person with certain characteristics.

Similarly, the **Internet lifestyle of a particular person**, which includes social activities such as chatting, publishing and/or sharing content on social networks, professional activities such as communicating via email, making audio/video calls and/or sharing and storing files on storage and synchronisation services/applications, as well as routine activities such as buying products, making payments, consulting websites and using applications, can be seen as a determinant of exposure to cybercrime (Van Wilsem, 2011).

Further, a person's lifestyle also influences their risk of engaging in illicit activities, offering the opportunity to engage in criminal behaviour (perhaps with deviant peers) and keeping them away from peer supervision and other protective relationships (McNeeley, 2015).

This theory was combined with the routine activity theory, described below, for a more general explanation of crime/victimisation (*idem*).

### 3.1.4. Routine Activity Theory

Following up from the lifestyle theory, the **theory of routine activities** seeks to explain the occurrence of crime by combining the following conditions:

- motivated offenders;
- suitable target/victim;
- absence of guardianship (Cohen & Felson, 1979 *cit in* Maimon & Louderback, 2019).

If one (or more) of these three conditions is absent, the likelihood of crime decreases (Phillips, 2015).

Regarding **cybercriminals**, the proximity of the victim to motivated cybercriminals increases the risk of victimisation (Van Wilsen, 2013 *cit in* Maimon & Louderback, 2019).

HIGHLIGHT | INFORMATION IN FOCUS:

The motivation for the practice of a cybercrime can be **situational**, namely by the presence of stimuli that, regardless of any personality traits, may lead to engagement in cybercrime (Briar & Piliavin, 1965 *cit in* Maimon & Louderback, 2019). These stimuli can be associated with the occurrence of **opportunity motivated crime** which, in the case of cyber-dependent crime, can include vulnerabilities in a given operating system, the absence of surveillance systems and/or the availability of unencrypted data. These circumstances reduce online offenders' risk of detection, which in turn increases the probability of occurrence of cybercrime (Willison & Siponen, 2009 *cit in* Maimon & Louderback, 2019).

The **suitability** of the target/victim is rationally assessed by the offender, through the value or desirability of the target, its visibility, inertia and accessibility (Felson, 2002 *cit in* Maia et al., 2016).

Also regarding the suitability of the target, in the case of cybercrime, given the accessibility and the number of users of (and on) the Internet, the opportunities for cybercrime are considered to be greater than the practice of crime in the physical world (Saridakis, Benson, Ezingeard & Tennakoon, 2016).

ICT and Internet usage levels seem to be an important indicator of **target suitability**, i.e. people with longer periods of ICT use are at greater risk of cyber-victimisation. The study by Wang and colleagues (2015 *cit in* Maimon & Louderback, 2019) has shown that, in fact, accessibility, visibility and exposure of a target can increase the risk of cyber-victimisation. Still within the scope of **suitability**, cybercrime is also more frequent in wealthier countries and, as such, with more users of (and on) the Internet (Kigerl, 2012 *cit in* Maimon & Louderback, 2019).

With regard to cybercrime directed at companies and organisations, the suitability of the target increases the risk of cybercrime. In this sense, cybercrime is more frequent during the working hours of the target companies or organisations, during which the number of available potential victims is higher (Kigerl, 2012 *cit in* Maimon & Louderback, 2019).

In turn, **guardianship** in the case of cybercrime and, specifically, cyber-dependent crimes, involves (Grabosky, 2016 *cit in* Maimon & Louderback, 2019):

- Police authorities;
- Government organisations responsible for the management and monitoring of cyberspace;
- Internet Service Providers, companies and industries that use different tools and practices to prevent cybercrime.

In terms of cybercrime, guardianship can be analysed from different dimensions (Bossler & Holt, 2009, Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019). Thus:

- the absence of **social guardianship** (e.g. parental supervision when children use the Internet) seems to be associated with an increased likelihood of cybercrime;
- although not unanimously accepted, **physical guardianship** (which includes the use of ICT security systems or software) is associated with reducing the risk of cyber-victimisation;
- the presence of **personal guardianship** (which concerns knowledge and skills of ICT and Internet use) reduces cybercrime

In conclusion, the theory of lifestyle and routine activities emphasises the idea that a **person's routine lifestyle activities and behaviours can increase their levels of suitability as a (potential) target of cybercrime** and their exposure to offenders, which, in the absence of guardianship mechanisms, increases the risk of victimisation and cyber-victimisation (Cohen, Kluegel & Land, 1981 *cit in* Phillips, 2015).

### 3.1.5. Other relevant approaches

In brief, **social learning theory** understands crime as a learned behaviour, like any other behaviour.

This learning process involves:

- interactions of an individual with others in a particular group;
- an individual's attitudes towards behaviour, including techniques, rationalisation and motivation to perform a behaviour;
- imitation, including observation and repetition of a certain behaviour displayed by other elements of the group;
- reinforcement, including rewards that promote the initiation and maintenance of the behaviour.

(Akers, 1998 *cit in* Marcum et al., 2014)

Social learning theory also seems an appropriate explanation for cybercrime as it understands criminal behaviour as learned, through a process of peer imitation and assimilated by positive reinforcement mechanisms, and **association with similar peers** seems to be related to involvement in cybercrime practice (Hutchings & Clayton, 2016 *cit in* Maimon & Louderback, 2019).

In this way, a progression can be observed from individual approaches or perspectives, associated with the psychological, emotional characteristics and cognitive processes of a given individual, to their interpersonal relationships, where it is also important to highlight the **involvement in more or less organised networks of deep web peers**, with its own **subculture and (hierarchical) structure**, as a risk factor for the perpetration of cybercrime (Macdonald & Frank, 2017 *cit in idem*). It should also be said that the maintenance of **loyalty in relationships** is pointed out in some studies as a motivation for involvement in cybercrime, particularly in the case of cyber-dependent crimes (Hutchings & Clayton, 2016 *cit in idem*).

Cybercrime can also be explained according to three dimensions (Thornberry, Krohn, Lizotte & Chard-Wierschem, 1993 *cit in* Peterson & Densley, 2017):

- **selection:** the cause of cybercrime is not the Internet itself, but rather the individual risk factors and criminal propensity present in people using the Internet, ICT and social networks;
- **facilitation:** the Internet and ICT have an effect on the facilitation of cybercrime, due to some of the propitious features of the online context, such as anonymity, lack/absence of guardianship and group processes (such as conformity to group norms);
- **enhancement:** which combines the effects listed above - selection and facilitation - explaining that the occurrence of cybercrime is associated with the **presence of individual risk factors in people most prone to the practice of cybercrime** and the aforementioned **characteristics of the Internet**, social networks and ICT that enhance the expression of criminal propensity.

# 3. CRIMINOLOGICAL AND VICTIMOLOGICAL PERSPECTIVES FOR THE UNDERSTANDING OF CYBERCRIME

## 3.2. The cybercrime victim and the risk factors associated with cyber-victimisation

As already discussed in this Handbook's section 1, the cybercrime's 'ecosystem' and its different forms of expression includes an often secondary or neglected part in the understanding of the criminal phenomenon: we refer specifically to **victims of crime**.

HIGHLIGHT | INFORMATION IN FOCUS:

In accordance with Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime[68], *victim* is defined as:

i. *a natural person who has suffered harm, including physical, mental or emotional harm, or economic loss directly caused by a criminal offence,*
ii. *family members of a person whose death was directly caused by a criminal offense and who have suffered harm as a result of that person's death.*

In other words, the **victim of a crime** is a person who, as a result of an act committed against the criminal laws in force, has suffered an attack on their life, physical or mental integrity, emotional suffering or material loss. Victims are also considered to be close relatives or dependants of the direct victim, as well as persons who have suffered some kind of harm when intervening to assist the victims or to prevent victimisation.

According to the *IVOR Report: Implementing Victim-Oriented Reform of the criminal justice system in the European Union*,[69] a report that reflects on research, scientific and empirical knowledge regarding the practical implementation of the rights of victims of crime in Europe, a clear definition, at least from a legal point of view, of the concept of *victim of a crime* not only contributes to better support and protection of victims, but also promotes greater **awareness and recognition of the victim's status** in the criminal phenomenon and the justice system.

At this point in the Handbook, we will try to give visibility to victims who, as a result of one (or more) cyber-dependent crimes and/or any crime enabled or facilitated by the Internet and ICT, have suffered any loss, be it physical, moral, mental, emotional or material. We will begin by addressing some of the risk factors associated with cybercrime.

**Risk factors**[70] relate to characteristics, conditions or variables associated with a given person that increase the probability of negative or undesirable outcomes (Reppold et al., 2002 *cit in* Maia et al., 2016).

They can be static or dynamic. Static characteristics or conditions of the person and/or their past are not changeable, such as sex, personal experiences of violence in childhood, or the loss of a relative. On the other hand, dynamic risk factors refer to characteristics, conditions or variables that are modifiable and increase the likelihood of a particular problem occurring.

[68] Complete document is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0029&from=PT

[69] Additional information on the reflection around the definition of the concept of victim of crime and other matters relating to their rights and its effective implementation is available in the full report at https://apav.pt/publiproj/images/yootheme/PDF/IVOR-Repot-WebVersion.pdf .

[70] For clarity, it is important to note that the concept of risk factor cannot be dissociated from the concept of **protection factor**, which refers to characteristics or conditions that may diminish the probability of appearance or occurrence of a certain problem.

Thus, by conceptualising cybercrime as a problem or negative result, **the risk factors** associated with cyber-victimisation are characteristics or conditions that can increase a person's probability or vulnerability to cybercrime.

Research is not particularly extensive in this field, as in many others associated with the understanding of cybercrime. Nevertheless, the following studies are highlighted.

### 3.2.1. Risk factors associated with socio-demographic characteristics

The association between **gender** and the risk of cyber-victimisation is not straigthforward, and it is important to consider at least the different types of cybercrime as well, otherwise the understanding of vulnerability to cybercrime will be diminished. Let's examine some of the available information.

Although there is no consensus, some studies point to the fact that women are more likely to be victims of cyber-dependent crime (Bossler & Holt, 2009, 2010, Ngo & Paternoster, 2011 cit in *Maimon* & Louderback, 2019). The same seems to be true for cyberstalking (Holt & Bossler, 2008), with higher prevalence rates affecting females, as well as for cyberbullying.

On the other hand, in the case of online sexual abuse and exploitation of children, although the proportion of female victims is higher than for male children, at least in the cases identified, the latter are usually the target of more serious, severe and intrusive forms of sexual aggression[71].

As far as exposure (namely of children and young people) is concerned, for example, to the content of hate speech online, the differences in the European average of exposure rates between children/teen girls and children/teen boys are minimal. The same scenario has been identified in the reception of self-produced sexual/sexting content, with very similar averages for both genders[72].

Likewise, **age** also reveals, in the studies and research conducted to date, an inconsistent relationship with the risk of cyber-victimisation (Bossler & Holt, 2009, Ngo & Paternoster, 2011 cit in *Maimon* & Louderback, 2019). However, some studies indicate that older people are, more often than other adults, victims of cyber-dependent crime, such as hacking (Leukfeldt & Yar, 2016 cit *in Maimon* & Louderback, 2019).

On the other hand, and in general terms, the younger population, as we will address below, has high rates of intensive use of ICT and the Internet, specifically use of social networks, which will result in greater vulnerability to cyber-victimisation compared to older and less frequent users (Staksrud, ÓLafsson & Livingstone, 2013 cit *in Näsi*, Oksanen, Keipi & Räsänen, 2015; Näsi et al., 2015).

With regard to **education**, there are studies that point to a possible negative relationship between

[71] Detailed additional information is available at https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database .

[72] See the results of the *EU Kids Online 2020: Survey results from 19 countries* at https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf .

the education level and cyber-victimisation, namely for hacking, *i.e.* higher levels of education will be associated with a lower risk of cyber-victimisation (van Wilsem, 2013 *cit in* Maimon & Louderback, 2019). However, as in the previous socio-demographic characteristics, the effect of this risk factor requires further investigation, given the still recent knowledge regarding the risk of cyber-victimisation associated with individual characteristics.

### 3.2.2. Risk factors associated with the use of the Internet and ICT

The concept of **technological literacy** refers to the awareness, knowledge and skills that enable a person to use the Internet, ICT and associated equipment and tools effectively, and to navigate digital environments (Holt & Bossler, 2013 cit *in Maimon* & Louderback, 2019).

It is therefore an important factor in determining the levels of risk and protection against cyber-victimisation. Internet and ICT skills and knowledge seem to reduce the risk of cyber-victimisation, also by providing the user with a greater ability to identify and act in situations where their online security may be at risk (Holt & Bossler, 2008).

There are several studies that indicate the existence of an increase in vulnerability to cyber-victimisation in different forms of cybercrime, such as hacking, malware and phishing, depending on the **levels of Internet and ICT use** (Yucedal, 2010; Leukfeldt & Yar, 2016; Reyens, 2015 *cit in* Maimon & Louderback, 2019). It seems that there is an association between the level of activity in ICT and cybercrime victimisation: people with increased usage of social networks and ICT in general in their daily activities also have higher levels of personal experiences of cybercrime victimisation (Butler, 2013). This finding is in line with the criminological theories already discussed in this Handbook.

HIGHLIGHT | INFORMATION IN FOCUS:

The increased risk of cyber-victimisation as a function of ICT usage levels should not be interpreted in a linear way, where the use of ICT and the Internet on its own increases the risk of cyber-victimisation.

It is mainly the **behaviours and type of activities performed when using ICT and the Internet** that are the main factors contributing to the increased vulnerability to cybercrime victimisation (Butler, 2013; Holt & Bossler, 2008).

This vulnerability will be addressed in more detail in the next section of this Handbook.

### 3.2.3. Behavioural vulnerability and its association with cyber-victimisation

HIGHLIGHT | STATISTICS IN FOCUS:

According to the data from the aforementioned transnational study *Health Behaviour in School-aged Children*, 35% of the school students surveyed consider themselves to be **very intensive users of the Internet and ICT**, i.e. they use these tools daily and for a significant part of the day.

Further, 1 in 10 school students report intensive use of the Internet and ICT to communicate with people they have met only through the Internet.

On average, around 7% of school students also reveal **addictive behaviours** associated with the use of the Internet and ICT, especially for female respondents.

As mentioned in relation to lifestyle theory and routine activity theory (see section 3.1. of this Handbook), a person's online lifestyle affects their risk of cyber-victimisation (Yucedal, 2010).

As noted by the theoretical approaches to criminology, the online lifestyle includes all **kinds of activities carried out on the Internet or through the Internet and ICT**, either in terms of social interactions and leisure activities, or actions and tasks associated with professional, educational or other occupations, and even routine tasks, including online shopping, making payments and even scheduling commitments and/or fulfilling obligations towards the State. The frequency and intensity of use of the Internet and ICT is also relevant.

Using the concept of online lifestyle, which is comprehensive, it becomes clear that the levels of cyber-victimisation risk is different depending on the activity carried out on in the Internet or through the Internet and ICT and for different routine usage.

Some activities, such as downloading freeware programs[73] or using file-sharing websites, present a higher risk of cyber-victimisation than other activities, such as checking emails or visiting online news channels. Similarly, people who engage in less secure online activities, such as visiting unknown websites and/or downloading music, videos, movies and/or games on unofficial platforms, are more likely to be the target of some form of cyber-victimisation (Choi, 2008, Moitra, 2005, Yar, 2005, 2006 *cit in* Yucedal, 2010). In turn, the use of a webcam, frequent usage of online shopping and the acceptance of friendship requests on social networks from unknown people/profiles increase the risk of cyber-victimisation, compared to the risk of cyber-victimisation evidenced by people without such Internet and ICT routine activities (Clarke, 2004; van Wilsem, 2011; Butler, 2013).

[73] Freeware refers to software or computer programs whose use does not require the purchase of a license/payment.

HIGHLIGHT | INFORMATION IN FOCUS:

Regarding online lifestyle and Internet usage behaviours, it is also important to note that **people with personal experiences of perpetration or involvement in cybercrime also present a higher risk of experiencing cyber-victimisation** (Choi, 2008, Wolfe et al., 2008, Bossler & Holt, 2009, van Wilsem, 2013 cit *in Maimon* & Louderback, 2019).

This increased risk of victimisation by persons involved in illicit activities is similarly found in *traditional* crime, and is associated with lifestyle, behaviour and differing levels of exposure to circumstances, contexts and persons/groups at risk (see summary of criminological theories in section 3.1 of this Handbook).

In this matter, and in the case of cybercrime, the aforementioned involvement and belonging to specific criminal subcultures are associated not only with the risk of cybercrime (Macdonald & Frank, 2017 cit *in Maimon* & Louderback, 2019), but also with that of cyber-victimisation, through exposure to deviant peers.

To understand better the relevance of behaviour in the use of the Internet and ICT and its association with vulnerability to cyber-victimisation, there is an urgent need to address the **disinhibition effect**, an important feature associated with the use of the Internet and ICT. This disinhibition process or effect results from the way in which the physical distance affects interaction or communication. The absence of direct contact in the communication process, the greater anonymity and the perception of greater control over the interaction process seem to contribute to an easier sharing of information, the free expression of emotions and thoughts and the adoption of behaviours that would not be shared, expressed and practised in the case of interactions taking place in conventional contexts (Suler, 2004; Martellozzo & Jane, 2017). This apparently advantageous disinibitory effect may contribute to exposure to situations and/or the adoption of online behaviours that increase vulnerability to cyber-victimisation (Agustina, 2015).

HIGHLIGHT | PRACTICES IN FOCUS:

In 1995, a working group of a company based in the United States of America developed a memorandum called *Netiquette Guidelines*, in which, for the first time, the concept of ***netiquette*** was used. It consisted of a set of rules of behavior, including communication rules and security standards, applicable to people and collective entities, with the purpose to ensure a safe and appropriate use of the Internet and its different communication tools.

The original document is available at https://www.ietf.org/rfc/rfc1855.txt .

In this sense, it is necessary to highlight the importance of **awareness, knowledge** and **control skills** in **relation to the form and type of personal information shared or shareable** on the Internet and, specifically, on social networks. In this respect, a significant association was identified between the perception of privacy risk , the perceived control regarding shared information and the information

sharing behaviour on social networks: people with higher levels of perceived control of shared/shareable information, share more carefully, perceive themselves as safer and are less likely to be victims of cybercrime (Hajli & Lin, 2014 cit *in* Saridakis et al., 2016).

## 3.3. Collective entities as targets of cybercrime

Cybercrime also has the potential to affect collective entities, crossing the barriers of individual victimisation addressed throughout this Handbook.

We refer specifically to situations where the targets of cybercrime are **corporations, multinationals, institutions and even government infrastructures** (Yucedal, 2010; Näsi et al., 2015).

These entities may suffer substantial losses as a result of cybercrime, either due to losing clients and/or compromised or stolen confidential information, or through immediate financial losses, which may even affect and harm individual clients, as well as future losses, associated with a decrease in client trust in the products and/or services they provide (Nykodym, Taylor & Vilela, 2005, 2005; Kratchman et al., 2008).

HIGHLIGHT | INFORMATION IN FOCUS:

The human element is also important in cybercrime targeting collective entities. We refer, namely, to the **role of professionals and staff** of those organisations and their **levels of implementation of organisational policies and measures of protection** against cybercrime, as well as their personal cybersecurity self-protective behaviours.

It is known that an adequate understanding of organizational vulnerabilities by professionals and staff has a positive effect on the levels of compliance with protection strategies and policies adopted by a given corporation or organization (Johnston & Warkentin, 2010 cit *in Maimon* & Louderback, 2019; Siponen et al., 2010 cit in *Maimon* & Louderback, 2019).

Cyberterrorism, summarily presented in sectiont 1 of this Handbook, is an example of a form of cybercrime that targets collective entities, since its intention, as previously indicated, focuses on the destruction and/or incapacitation of critical infrastructures for the functioning of a society or a state, and not necessarily on the damage to individual citizens (which can also occur following the attack).

Also, in this field, it is important to note the concept of hacktivism, which results from an intersection between political activism and ICT, where hacking supports political purposes or causes (Yar & Steinmetz, 2019).

# 3. CRIMINOLOGICAL AND VICTIMOLOGICAL PERSPECTIVES FOR THE UNDERSTANDING OF CYBERCRIME

HIGHLIGHT | INFORMATION IN FOCUS:

Anonymous, the international decentralized movement of hacktivism, which emerged on the Internet in the 2000s and is known for its practice of hacking and DDoS (see section 1.3 of this Handbook for more information on these forms of cybercrime), has been associated with several attacks against government infrastructures, multinationals, financial institutions and religious entities.

The movements' objectives are not clear, but they claim to fight against censorship and oppression and in favour of the promotion of freedom of expression.

# 4. THE COSTS AND IMPACT OF CYBERCRIME

In this section, we will cover a set of symptoms and indicators of the impact of cyber-victimisation, with the caveat that, given the multiplicity and vast scope of phenomena under analysis, the consequences presented below will always be reductive and generic, not contemplating the individuality of each particular and personal experience of cyber-victimisation.

We will also seek to address the financial and economic costs associated with cybercrime, considering that although they may directly and/or indirectly affect individual victims, it is common that their consequences are also reflected in costs to collective entities, which are attractive targets of cybercrime.

## 4.1. The victim of cybercrime and the consequences of the experience of cyber-victimisation

The impact of cybercrime on the victim is very variable, being aggravated or attenuated according to a set of variables:

- **Individual variables**, namely socio-demographic characteristics and Internet usage skills (already addressed in the risk factors associated with cyber-victimisation in section 3 of this Handbook);
- **Variables associated with the cybercrime** itself, including the type of cybercrime and the level of underlying aggression, the duration of the cyber-victimisation, the reach of dissemination or level of publicity of the cyber-victimisation and, where applicable, the relationship with the cybercrime perpetrator (e.g. in situations of cyber-victimisation in interpersonal relationships);
- **Variables associated with the support network**, which includes the formal support network (i.e. the resources and services available from the justice, health, security and social security systems, and as civil society organisations), as well as the informal support network, namely family and friends.

### 4.1.1. Physical, psychological and emotional consequences

Existing studies on the impact and consequences of cyber-victimisation are scarce and, with few exceptions (e.g. Jansen & Leukfeldt, 2018), have focused mainly on analysing the impacts of particular forms of cybercrime, such as crimes made possible by the Internet and ICT, possibly due to their relational or interpersonal component.

In generic terms, it is considered that the consequences experienced by cybercrime victims are not significantly different from the consequences experienced by victims of what we will call *traditional* crimes. The consequences and reactions often pointed out are: loss of confidence; guilt; shame; anger and frustration; anxiety; fear and sadness; feelings of insecurity, powerlessness and disappointment (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020). The emotional impact of certain

types of cybercrime can be as severe as their financial consequences (Modic & Anderson, 2015). Victimisation can also change the way victims perceive themselves and how they understand and attribute meaning to the world around them, including the reduction in levels of self-confidence and trust in others (Jansen & Leukfeldt, 2018), and then can evolve into physical effects such as insomnia, nausea, and/or weight loss (Cross et al., 2016).

In cyberstalking situations, fear, distress and concern felt by victims are often identified, alongside emotional, psychological and behavioural consequences (Holt & Bossler, 2008). Fear could be related to the offender, but it could also be associated with the fear of loss of reputation, because of the possibility of personal and private information being disclosed online and, as such, reaching a large audience or high levels of publicity. Symptomatology of anxiety, including re-experiencing the incidents, and substance abuse are also associated with cyberstalking victimisation. Along with emotional and psychological consequences, signs of physical malaise may emerge, including somatisation[74], sleep disorders, tiredness or excessive weakness, appetite problems, headaches, and nausea (Davies, Clark, & Roden, 2016).

In cases of cyberbullying, we can list suffering, low self-esteem, sadness, anger, loneliness and frustration, as well as somatic disorders, depression and suicidal ideation as frequent negative effects on the victim's psychological and emotional functioning. Cyberbullying also has consequences in the social and educational functioning of the child or young victim and is associated with feelings of inefficiency, isolation, school absenteeism, and decline in academic performance (Beran & Li, 2007, Kowalski & Limber, 2013 cit in *Arafa*, Mahmoud & Senosy, 2015; Wang et al., 2011 cit in Arafa *et al*., 2015).

Furthermore, retrospective studies have identified a wide range of negative consequences from the emotional and psychological functioning associated with sexual abuse in childhood, including: educational and occupational difficulties, aggressiveness and involvement in criminal activities. As for cyberbullying situations or of child sexual abuse and exploitation's, symptoms such as fear, anxiety, aggressiveness and irritability, as well as sleep disturbances and regressive behaviours[75], can appear. Similarly, consequences may also include a decline in school performance, school absenteeism, as well as the adoption of inappropriate sexual behavior (Roopesh, 2016 *cit in* APAV, 2019).

Despite, a focus on the sexual abuse and exploitation of children and their consequences[76] being out of scope for this Handbook, given the atypical nature of some of those situations, we present below a brief summary of the aforementioned maladjusted sexual behaviours that may arise as consequences/ effects of exposure to sexual violence.

[74] Somatization refers to the manifestation of physical symptoms as an expression of emotional and psychological problems, without apparent medical/physical reason.

[75] Regressive behaviours refer to the regression in developmental acquisitions already achieved by the child, which may include, for example, enuresis (involuntary loss of urine), encoprese (involuntary defecation) and language/communication regressions.

[76] For detailed additional information on sexual violence against children, please see: APAV (2019). *CARE Handbook - support for children and young people victims of sexual violence (2nd edition revised and expanded)*. Lisbon: APAV.

**Table I-9: Sexual behaviours that may arise as a consequence of sexual violence victimisation experiences**

**Sexualised expression of affection**

- Inappropriate touching other children and young people's sexual organs (particularly children and young people of ages different than their own and/or with whom the child or young person has no previous relationship of trust)
- Excessive or inappropriate touching of adults
- Seductive conducts towards adult people

**Early sexual language**

- Use of sexual terms indicative of unexpected knowledge about sexuality for their age group

**Compulsive masturbation and/or extreme autoerotic behaviour**

- Persistent masturbation even when requested to stop or being censored by adults (e.g. application of consequent punishment for the practice of masturbation)
- Masturbation in public places and/or near other people

**Staging or simulating explicit sexual episodes and/or interactions**

**Sexual behaviour that creates unease in oneself and in others (especially in peers)**

- The sexual conduct causes physical pain in themselves and in the peers with whom they seek to carry out sexual acts
- The sexual conduct invades the peers' privacy, is against their will and results in peer complaints

**Sexual conduct conceived as a form of reciprocation/appreciation of affection and/or material goods**

**Constant concern about sexuality**

It is thus clear that situations of sexual abuse and exploitation of children via the Internet affect their healthy development, including sexual development, as well as their identity. Because of the high risk of continued victimisation associated with child sexual abuse and exploitation, the impact of the experience is likely to increase in severity and the consequences are likely to persist into adulthood (Frothingham et al., 2000 *cit in* Sigurjonsdottir, 2013).

Also, in situations of online hate speech there is a double impact: the impact of the content/message on the victim, but also the impact arising from the underlying message that the same content is intended to convey (that the victim and the group to which they belong or are perceived to belong are not tolerated by society). The anonymity enabled by the Internet and ICT to offenders contributes to the perpetuation of online aggression, and thus intensifies the emotional and psychological suffering of the victim. In addition, anonymity's potential for amplification and social 'validation', particularly when the spread takes place on social networks, aggravates and intensifies the negative impacts on the victim's emotional, psychological and even social functioning (McGonagle, 2013).

In the case of cyber-dependent crimes such as hacking, spamming or online scams, the impacts on emotional and psychological well-being are largely underestimated and are usually discussed as low-impact crimes (Button, Lewis, & Tapley (2014a cit *in Jansen* & Leukfeldt, 2018). However, beyond the financial consequences associated with these forms of cybercrime, there are studies that point to the occurrence of emotional and psychological discomfort symptoms, such as fear and anxiety, as well as physical symptoms such as sleep problems and palpitations (Jansen & Leukfeldt, 2018).

### 4.1.2. Financial consequences

The financial damage suffered by victims of cybercrime depends mainly on the forms of cybercrime they have been subjected to (Butler, 2013).

Therefore, there may be direct financial consequences of cybercrime, as well as indirect consequences, that may include, for example, other costs incurred by the victims as a consequence of the act they were subject to, such as the waste of time, the loss of working hours, increased expenses with health, travel and telecommunications costs, the need for replacement of IT equipment and/or failure to comply with contractual agreements (Leukfeldt et al., 2019). There are cybercrimes which consequences for the victim also include the need to change their routines, which may imply the adoption of protection measures and the implementation of more effective cybersecurity mechanisms, but also more significant changes in lifestyle and daily activities, including moving house, change of place of work/study or others, which obviously entail financial costs.

On the other hand, the costs that entities bear as a response or consequence of being a cybercrime target , an area reviewed in section 4.3 of this Handbook, are ultimately reflected at the individual level, on the online consumers or users of a given product, good or service (Das & Nayak, 2013).

### 4.1.3. Fear of cybercrime and perceived risk of cyber-victimisation

**Fear of crime** can be defined as an emotional reaction to crime and/or to symbols associated with it, while **perceived risk** constitutes a cognitive judgment through which people assess their own risk or probability of victimisation, based on their personal experiences, social context and circumstances, which in turn is reflected in fear of crime (Ferraro, 1995, Rontree, 1998 *cit in* Yucedal, 2010).

It follows that **personal experiences of victimisation** can increase perceived risk of (re)victimisation and consequently fear of crime. These cognitive processes are not necessarily negative, as they can promote the adoption of safety and protection measures and behaviours (Rountree & Land, 1996, cit *in idem*).

Thus:

- A person who has already been a victim of crime or who consider themselves at risk of victimisation may **adopt more safety and protection behaviours**, including restrictions in social activities/ interactions or changes in daily routines, as well as the use of protection tools and mechanisms;
- A person who has already been a victim of crime may perceive themselves **to be at greater risk of (re)victimisation** and, as a consequence, have higher levels of **fear of crime** than people without prior experience of victimisation (Hindelang et al., 1978, Cohen & Felson, 1979, Ferraro, 1995, Goodrum, 2007 cit *in idem*).

These **cognitive processes for assessing the perceived risk of victimisation also apply to cyber-victimisation**. The perceived risk of cyber-victimisation, as a result of cognitive processes that include analysis of personal experiences of previous cyber-victimisation (if that is the case) and of victimisation/crime clues arising from online lifestyle, may lead to behavioural responses aimed at greater protection. This can include putting in place cybersecurity measures/mechanisms (such as anti-virus and firewall programs[77]) and changing Internet and ICT usage behaviours (Yucedal, 2010).

Ultimately, the perceived risk of cyber-victimisation also impacts the levels of **vulnerability to cyber-victimisation**, since, at the outset, if a person perceives themselves as being at risk of cyber-victimisation, they will more likely to adopt behaviours and measures geared towards ensuring cybersecurity, which will contribute to reducing the risk of cyber-victimisation.

HIGHLIGHT | STATISTICS IN FOCUS:

According to the data from the aforementioned Eurobarometer 423, respondents expressed **high levels of concern about cybersecurity and the risks of cybercrime**.

Here are some of the main results:

- The majority (85% of respondents) agreed that the **risk of cyber-victimisation is increasing**.
- 73% of respondents were concerned **that their online personal information is not kept secure**.
- The types of cybercrime that respondents are most concerned about are, in decreasing order: **online identity theft** (68%), **malware** (66%), **online scams** (between 56% and 63%), **hacking** (60%) and **spamming** (57%). Also, about half of those surveyed were concerned about the accidental discovery of **online child sexual abuse and/or exploitation material** (52%) and the accidental discovery of **hate speech** content/material (46%).

Despite these concerns, some 74% reported being **able to protect themselves against cybercrime**.

[77] Firewall refers to software and/or hardware that is intended to protect the computer/equipment and network from unauthorized access.

## 4.2. From the consequences to the needs of cybercrime victims

In general, the needs of victims of cybercrime are relatively similar to the needs of victims of other more *traditional* forms of crime, and different areas of needs can be identified (Leukfeldt et al., 2020).

While the needs more or less common to victims of any form of crime can be listed, there will be specific needs that also differ according to the type of victimisation and time scale (i.e. the needs of a cybercrime victim immediately after the cybercrime experience will be distinct from the needs identified some time after the cybercrime occurred).

In addition, the needs of crime victims also depend on the victim's personal characteristics, their social environment and the consequences of the specific cybercrime (Huang, 2018, Wood et al., 2015 *cit in idem*).

The table below summarises some of the needs identified by the victims of cybercrime and which will be caused by the cyber-victimisation experience (Cross et al., 2016; Leukfeldt et al., 2020). Its content is not exhaustive, given the scarcity of research on this subject.

**Table I-10: Needs identified by cybercrime victims**

| Emotional and psychological needs | Criminal-proceedings and information related needs | Practical and financial needs |
|---|---|---|
| • Recognition as a victim of a crime<br>• Recognition of the cyber-victimisation experience<br>• Need to tell their experience and be heard/listened to<br>• External acknowledgement (informal social contexts and authorities) of the experience of cyber-victimisation<br>• Have qualified and confidential support after the cybercrime experience<br>• Recovery from the emotional and psychological consequences of cybercrime<br>• Access to professional/qualified support | • Information on existing support resources/structures and how to request help<br>• Support in reporting and formalising the complaint<br>• Receive information about the cybercrime perpetrator, the investigation and trial<br>• Receive information on the outcome/result of the criminal proceedings<br>• Reparation for the crime | • Support in removing content related to the cybercrime from the Internet and ICT<br>• Support in liaising with banks, Internet Service Providers and other platforms<br>• Support in re-establishing security (preservation of physical integrity) and preventing re-victimisation<br>• Protection/shielding from the cybercrime perpetrator<br>• Financial needs associated with lost assets/information<br>• Monetary compensation for cybercrime losses |

The way in which the institutional responses provided by various systems and structures, such as the criminal justice system, the health system, the social support system, Internet Service Providers and Industry/Tecnhology, and even civil society organisations, intervene or take action, with a view to meeting the needs of victims of crime and victims of cybercrime in particular, may give rise to **secondary victimisation**. This is a second form of victimisation, caused by the inadequate response provided by these systems and structures and their discrepancy with the interests, needs and rights of victims.

HIGHLIGHT | PRACTICES IN FOCUS:

In what regards institutional cooperation, as an example, WePROTECT Global Alliance proposes a coordinated national response to online child sexual exploitation and abuse.

The proposed model acknowledges that online child sexual exploitation and abuse cannot be addressed in isolation and a wider set of capabilities to prevent and tackle it are required to be in place to ensure a complete national response.

Additional information at https://www.weprotect.org/.

The difficulties of different systems/services and institutional structures in responding to the needs of victims of cybercrime (*idem*) may be due to the following constraints:

- Insufficient human and material resources;
- Ignorance of the victims' needs and rights or structural difficulties in implementing them;
- Need for specialised training/knowledge for contacting and intervention with cybercrime victims;
- Difficulties associated with the criminal proceedings, including identification of a suspect, formalisation of a complaint, investigation and prosecution.

## 4.3. Financial and economic costs of cybercrime

Cybercrime has various costs to different entities, particularly when targeting collective entities. The magnitude of the economic and financial costs of cybercrime varies according to the sector, the organisation's size, the information assets and the severity of the form(s) of cybercrime used (Gañán, Ciere & van Eeten, 2017).

Cybercrime, when targeted at collective entities, namely corporations and organisations, aims, especially in the case of larger entities, to compromise their information assets. Smaller entities, on the other hand, seem to be less attractive targets for cybercrime (Gañán et al., 2017).

However, when we talk about the economic and financial costs of cybercrime for entities, many of these impacts are **intangible effects** and not exactly the loss of real money. While the need for comprehensive monetary estimates is understandable, the economic and financial impact of cybercrime is difficult to measure, as some of the effects can be monetised based on the available empirical data, but many of them are not (*idem*).

The various types of costs associated with cybercrime can be classified as costs in anticipation of cybercrime, as a consequence of cybercrime and in response to cybercrime (*idem*).

Thus, the costs in anticipation and costs as a consequence may include the costs (before and/or after) with **identifying risks**, building **cyber-security operating procedures** and acquiring cybercrime **protection software and hardware**. These costs may also include specialised consultancy on cybersecurity, as well as costs associated with testing, monitoring and regular updating of cybersecurity risks, procedures and systems (Das & Nayak, 2013).

The response costs will include all **public or private sector expenditures and efforts in the fight against cybercrime**, also borne by society, including the costs associated with the contributions of the criminal justice system to investigate and combat cybercrime (Gañán et al., 2017).

HIGHLIGHT | INFORMATION IN FOCUS:

**Impact of cybercrime on user confidence**

Anticipation costs are crucial to ensure user and consumer confidence and security on the Internet and ICT.

The convenience, accessibility and security associated with the use of the Internet and ICT for the consumption and purchase of products, goods and services are at the basis of consumers' preference for e-commerce and online activities, compared, for example, with physical shops.

Cybercrime undermines the advantages associated with the use of the Internet and ICT, increasing the **perceived risk indices** by online users and consumers, reducing confidence levels and thus contributing to changing attitudes towards online consumption.

If the perception of risk towards cybercrime undermines the confidence of users or consumers in the use of the Internet and ICT for certain activities, the attractiveness of online platforms for the consumption and purchase of products, goods and services decreases, which in turn can change online habits and behaviour (Saban, McGivern & Saykiewicz, 2002; Smith, 2004; Saini, Rao & Panda, 2012).

# PART II
# INTERVENTION

# PART II
# INTERVENTION

# 1. THE ROLE OF THE PROFESSIONAL IN SUPPORTING VICTIMS OF CYBERCRIME

This chapter addresses the importance and role of the professional supporting victims of cybercrime and the competencies and skills required to perform such functions. We also explore the psychosocial risks of the intervention with victims of crime, focussing on victims of cybercrime.

## 1.1. Personal competencies

Supporting victims of crime, particularly cybercrime, requires a set of essential professional support skills.

**Personal competencies** pertain to the professional's personal characteristics and personality and how they fit with the support functions and tasks. These are key in any care profession, and are therefore particularly crucial for professionals who work in direct contact with and support people in difficulty or in crisis (APAV, 2013), such as victims of cybercrime.

The main professional competencies for support and intervention with victims of crime - such as empathy, openness and availability - are addressed below (Pessoa, from Mota Matos, Amado & Jäger, 2011).

In addition, **the professional should also be able to manage and establish positive interpersonal relationships** when supporting victims of crime. This includes contact and interaction with victims, their relatives and friends, as well as liasing with professionals and partner organisations involved in the support and intervention with the victim. This relational dimension – managing human relations – includes the capacity for **peaceful resolution of interpersonal and/or interinstitutional problems and positive stress management**. These are good indicators of the capacity to relate to others, especially in such a complex and demanding intervention, where the professional can face constant adversity (APAV, 2013; APAV, 2017).

Similarly, **emotional self-management** is also a key competence - this is the ability to manage and regulate one's emotions in stressing, frustrating and demanding situations that are different from everyday life (APAV, 2013). Contacting and conducting interventions with victims of crime involves high levels of emotional engagement, which need to be quickly triggered to deal with the experiences of violence/crime shared by the victims, to deliver support (and cope with the stress and frustration associated with each case) and to cope with the impacts on the professionals' emotional balance (APAV, 2017).

The professional should also show **tolerance and respect for cultural values and differences**: regardless of any victim's characteristics or attitudes, the professional's approach should always be open and accepting. Neutrality and impartiality are fundamental for delivering support effectively, and professionals should try to manage and control their personal values and beliefs when supporting any victim (*idem*). Related to this dimension, at the basis of any support process with victims of crime, is the **respect for human dignity**, and it is fundamental to unconditionally accept the victim as a human being, simultaneously similar to oneself, but also as unique and individual.

Last but not least, it is important to mention two basic dimensions when contacting and supporting victims of any crime:

- **Compassion and Empathy:**

  The ability to put oneself in the *other person's shoes* or to imagine oneself as that person in that situation is fundamental when contacting, supporting and delivering interventions with victims of any crime. The ability to see things from the victim's perspective, to be sensitive to the situation experienced by the victim and to sense and understand the victim's feelings and meanings attributed to the crime are important in establishing a **supportive and trusting relationship between professional and victim** and can be an important aid to the success of the support and/or intervention.

  Empathy does not mean that the professional should cry or be moved by what the victim describes about the crime situation; what is important is the professional's capacity for emotional self-management. This balance is very important as it helps the victim of crime acknowledging the professional as a point of reference, as someone who is prepared and qualified for this work (APAV, 2017; APAV 2019).

- **Vocation:**

  This is more a personal condition rather than a competence – embracing values of social solidarity is very important for engaging with support, information and/or intervention with victims of any crime (APAV, 2017).

## 1.2. Core and specific technical competences

In addition to the personal competences mentioned above, the professional who contacts and provides support to victims of crime and, in particular, of cybercrime, must be properly qualified for this purpose and functions. The professional should also be embedded in a specific institution, be it public or private, governmental or non-governmental, social volunteering or not (APAV, 2013).

**Basic training** (i.e. academic qualifications) in a given scientific area (such as social sciences, for example, or another area, depending on the type of support provided by the professional and/or the support organisation) and accumulated **professional experience** are important requirements for the intervention with victims of any crime, including cybercrime, in its different forms (APAV, 2017).

Thus, it is expected that, according to the identified victim's needs and the nature of the support requested, certain professionals will be more suitable to best meet the interests, individual needs and rights of different victims of crime. It is therefore clear that, for example, legal support should be provided

by professionals specialised in the field of law, and psychological support should be provided by qualified psychologists[78].

It is also important to stress that, considering the diversity of needs and consequences usually felt by the victims of cybercime[79], there's a requirement for **interdisciplinary support and intervention** which may involve the action of professionals with different technical backgrounds, as well as the intervention of different organisations. A network-based approach involving professionals and organisations with different expertise and know-how and from different intervention areas/sectors contributes to a better intervention with each cybercrime victim and to adequately meet their individual needs.

In addition to higher education and professional experience, the professional who contacts or supports victims of cybercrime should also have **specific**, regular and continuous **training** in intervention with victims of crime and cybercrime, as well as cybercrime as a specific area of knowledge (APAV, 2013; APAV, 2017). In this specific training, the following key contents should be considered: the theoretical, criminological and victimological understanding of the different forms of cybercrime; knowledge about the consequences, impacts and dynamics of cybercrime, as well as the needs and rights of victims; the legal framework and existing legal and social responses; cybersecurity; among other contents.

Additionally, given the nature of cybercrime and the tools through which cybercrime is committed, contacting and supporting victims of cybercrime also requires **knowledge and specialised training regarding the Internet, ICT and other equipment**, both in terms of how these work and the communication tools supported by the Internet (which include social networks), and in terms of how they can be used to commit crimes and/or how they can be targets of cybercrime themselves (Bloom, 2007, Poh et al., 2013, Trepal et al., 2007, Mallen, Vogel, & Rochlen, 2005 cit *in APAV*, 2017). The professional's **information and technological proficiency** is fundamental for their ability to follow the constant evolution of ICT, the trends of communication through the Internet, as well as the permanent and consequent mutation of cybercrime.

No less important are **communication skills** in contacting and supporting victims of cybercrime, namely, knowing how to listen, but also having the ability to transmit clear and intelligible information and messages, as part of the support process, around topics which are quite complex (Person et al., 2011). Communication and empathy, as the basis of the support process and the relationship between professionals and victims of cybercrime, will be dealt with in more detail in the following sections of this Handbook.

[78] See Part II, Chapter 3, section 3.5 of this Handbook for information on the key aspects of expert support for victims of cybercrime.

[79] See Part I, Chapter 4 of this Handbook for more information on this subject.

## 1.3. Psychosocial risks from contacting and supporting victims of cybercrime

Professionals contacting, supporting and/or delivering interventions with victims of crime present high levels of **physical and emotional tiredness, psychological suffering and occupational stress** – this is due to these functions and by the need for direct contact with people in situations of particular vulnerability and fragility (emotional, and also physical) caused by victimisation and cyber-victimisation. Not only are these professionals exposed to other people's personal experiences of victimisation, but they are also confronted with the frustrations associated with the imbalance between the expectations of solving/addressing the problems and needs presented by the victim and the functioning and resources provided by the system and institutional structures. In addition, for the professional supporting cybercrime victims, beyond the *conventional* exposure to victims' reporting of their personal experiences of victimisation (see the following sections in this Handbook, where we will detail the importance of collecting information), another potentially stressful or traumatic dimension refers to the need to view content such as images, photographs and/or videos, of a criminal nature associated with the forms of cybercrime that committed against the victim being supported. This content may be of a markedly aggressive, violent and even sexually explicit nature and takes place when, for example, supporting children and young victims of sexual abuse and/or exploitation through the Internet, supporting victims of cyberstalking or supporting victims of sexual extortion or non-consensual dissemination of images and videos e.g in situations of revenge porn[80]). Continued exposure to this type of potentially traumatic content may affect the support professional's well-being and mental health (McCann & Pearlman, 1990).

It is not uncommon, therefore, for burnout to occur, which is defined succinctly as a syndrome (or constellation of symptoms), which includes symptoms of **emotional exhaustion, depersonalisation**[81] and **low personal fulfillment**, as a response to stressful work situations (Campos, Jordani, Zucoloto, Bonafé & Maroco, 2012).

The following table summarises some preventative organisational measures and individual behaviours when contacting or supporting victims of cybercrime, with a view to preventing psychosocial risks associated with supporting victims of crime and cybercrime.

[80] For detailed information on these forms of cybercrime, please refer to Part I, Chapter 1 of this Handbook.

[81] Depersonalization is defined as the process of dehumanization in the treatment/contact with the other, manifested through interpersonal interactions devoid of affectivity and empathy.

**Table II-1: Measures to prevent psychosocial risks associated with supporting victims of crime and cybercrime**

| Support service provider's organisational measures | Support professionals' individual behaviours |
|---|---|
| • Promote an organisational culture of openness to feedback and sharing of experiences<br>• Provide professionals with access to internal and/or external psychological support mechanisms or responses<br>• Implement counselling mechanisms (individual or group delivery) to promote well-being of support professionals<br>• Hold regular meetings to discuss and share experiences/ cases among peers/team/supporting professionals<br>• Ensure workspaces are equiped with material and logistical resources required for the work activities and for promoting well-being<br>• Promote leisure and recreational activities not related to the usual work tasks and functions | **Self-care behaviors:**<br>• Doing physical exercise<br>• Having leisure activities<br>• Following basic health standards, and keeping a balanced diet and good sleep hygiene<br>• Keeping in touch with family and friends<br>• Acknowledging and respecting the limits of body and mind<br>• Ensuring periods of rest and disconnection from work, through pleasurable activities<br>• Using relaxation and meditation techniques<br>• Having contact with nature<br>**Intervention techniques:**<br>• Having access to psychological support, provided by the support organisation either in-house or externally<br>• Participating in individual and/or group counseling (team/pairs) |

# 2. KEY ASPECTS FOR CONTACTING WITH VICTIMS OF CYBERCRIME

This chapter covers a set of general guidelines for the initial contacts with victims of cybercrime, a step taking place before a more structured and qualified intervention, and should apply to any organisation contacting with victims of cybercrime.

To this end, we highlight key dimensions for establishing a relationship of trust between the victim and the support professional, including communication and empathy, but also the collection of information and how it will guide any subsequent intervention with the victim. This chapter ends with an approach to the care of children and young people victims of cybercrime, given their particular vulnerability.

## 2.1. General guidelines for contacting with victims of cybercrime

Seeking support can represent a key and determining moment for a victim of cybercrime's emotional and psychological recovery and for the restoration of normality in their lives.

However, as in other crimes and also in situations of cybercrime, only a small proportion of victims, whose exact size is not known, choose to seek formal support, particularly from victim support services and responses. Despite the frequent reluctance to seek support (Cross et al., 2016), for reasons that intersect with those of not reporting cybercrime[82], as a rule, the request for support will depend on two conditions: that the victims of cybercrime recognise themselves as victims of a crime and that they assess the cybercrime suffered as serious (De Kimpe et al., 2020).

We present below some global guidelines for the professional's actions when supporting victims of any crime, including victims of cybercrime (Winkel, 1991; Machado & Gonlçalves, 2003 cit *in APAV*, 2013; Cross, Richards & Smith, 2016; Wedlock & Tapley, 2016; De Kimpe, Ponnet, Walrave, Snaphaan, Pauwels & Hardyns, 2020).

[82] See Part I, Chapter 1, section 1.4 of this Handbook for more detailed information on the difference between cybercrime reported and those actually committed.

**Quadro II-2: Orientações gerais para o contacto com vítimas de cibercrime**

| Objectives | Attitudes |
|---|---|
| **Acknowledge the complaint/report** | Acknowledge the victim's the courage to seek support and disclose their personal experience of cyber-victimisation. |
| **Respect the victim's pace and promote their sharing their experience** | Use preferably open questions, such as "what do you have to tell us?", promoting a safe space/ context for the free sharing of information.<br>Respect and promote emotional ventilation, as well as moments of greater fragility and emotionality associated with sharing the experience of cybercrime.<br>Clarify/question, without pressure, when the information provided by the victim is unclear or insufficient.<br>Respect the victim's timings, breaks and silences, including hesitations in sharing information. |
| **Validate the experience** | Empathetic listening, demonstrating that you are listening and understanding what is being said and valuing the reactions, emotions/feelings, behaviours, thoughts and meanings attributed by the victim to their victimisation/ciber-victimisation experience.<br>Demonstrate that you believe what the victim is telling you about what happened to them, without judging it.<br>Normalize the victim's reactions. |
| **Reestablish control** | Provide clear information, focussing on essential information to the victim about what happened and the next steps to adopt, through simple and clear language, adjusted to the victim's characteristics.<br>Do not take over the victim's decision-making, accept the victim's decisions without judging them and support their implementation/activation, so that the victim can re-establish control over their life.<br>Respect the victim's choices. |
| **Break with the idea of 'unique vulnerability'** | Provide information on the crime and its prevalence. |
| **Prevent blame** | Do not criticise.<br>Frame the victim's reactions in the emotional context associated with the crime.<br>Value previous protection attempts, even if they may have been ineffective.<br>Avoid using expressions like "why not..." and "you should have...". |
| **Prevent avoidance and isolation** | Recommend the progressive resumption of activities, including Internet and ICT use habits.<br>Encourage increased involvement in previously enjoyable activities, especially offline activities.<br>Mobilize social support.<br>Avoid overprotection by family and friends (without neglecting the safety of the victim). |
| **Promote emotional and cognitive processing of the experience** | Do not advise the victim to 'forget everything' and advise people close to them not to do so.<br>Suggest the victim to share feelings and fears with those they trust, advising those close to the victim to keep available to listen, without pressing the victim to share their experience. |
| **Prevent new crimes** | Discuss security and cybersecurity strategies.<br>Raise awareness of the risks associated with the use of the Internet and ICT by promoting the implementation of cybersecurity mechanisms and the adoption of personal protective behaviours when using the Internet and ICT.<br>Draw up, if necessary, a protection plan with the victim (particularly in situations where cyber--victimisation is accompanied by victimisation in *traditional* contexts). |
| **Involve significant people in the recovery process** | If the victim is willing and with their permission, involve family and/or friends in the recovery process, requesting their help to support the processing of the experience and to prevent new crimes, avoidance and isolation. |

We also present below a systematisation of appropriate practices and common mistakes to avoid in the contact with any victim of crime (APAV, 2019b).

**Table II-3: Good practices vs mistakes to avoid in the contact with cybercrime victims**

| Good practices in the contact with the victim of cybercrime | Mistakes to avoid in the contact with the victim of cybercrime |
|---|---|
| To believe the victim's account. | Not believing the victim's account. |
| Encourage the victim to talk about the cyber-victimisation situation, but without putting pressure on them. | Taking over the victim in decision-making, an error usually identifiable by expressions such as "You should not...", "You must...". |
| Respect confidentiality, taking its limits into account. | Making decisions without the victim's prior consent. |
| Do not judge. | Give the victim a false sense of security, promote unrealistic expectations about the professional's role, about the resolution of the situation or about the victim's needs, which can be identified through verbalizations such as "Don't worry. Everything will be fine." |
| Respect the victim's reading of their specific situation, even if it differs from the professional's view. | Minimize the problem and its impact. |
| Normalise the cyber-victimisation experience and the associated reactions, emotions, feelings and thoughts. | Adopting a position of hyperprotection towards the victim. |
| Explain to the victim that there are other people experiencing similar situations, breaking the perception of being a 'unique case'. | Demonstrate excessive interest in details of cyber-victimisation that the victim is unwilling to disclose (or is not yet prepared to disclose at that time). |
| Transmitting to the victim that they are not responsible for the situation, helping them to deal with possible feelings of self-guilt. | Show little time and/or availability to the victim and for listening, for example, through non-verbal manifestations of restlessness and/or interruptions to their speech. |
| To help the victim in their decision-making process, showing each options' advantages and disadvantages to support making informed decisions. | Proposing interpretations or diagnoses for the victim's reactions, emotions/feelings and thoughts in relation to their experience of cyber-victimisation, which can be conveyed in expressions such as "You are doing this because...". |
| Assess the risk of cyber-(re)victimisation and the victim's needs, provide appropriate support, depending on their situation, and/or referral to the services and/or organisations providing support. | Offer solutions, without involving the victim in the decision--making process. |
| Be prepared to intervene in a crisis situation. | Use humour inappropriately or make unnecessary self-revelations as strategies for establishing a relationship of trust. |

## 2.2. The importance of communication and empathy

**Empathy**, as mentioned above, is characterised by the ability to understand the other's perspective and to perceive and apprehend their current feelings, what they felt when experiencing cyber-victimisation, what they think or thought about the event, as well as the ability to demonstrate understanding and

validation of reactions such as discomfort and uneasiness or others, following, more or less immediately, the cybercrime.

The professional's empathy towards the victim and their experience of cyber-vitimisation is very important for **establishing a relationship of support and trust between the professional and the victim**, and fundamental for the successful implementation of the objectives listed above (see Table 2).

Playing a **crucial role in human communication**, as it facilitates the communication process, empathy encourages the victim to share, including information and evidence, which will contribute to the success of the support process, to the victim's recovery and to meeting their needs, but also benefits the criminal procedures (De Vignemont & Singer, 2006; Sommers-Flanagan & Sommers-Flanagan, 2014, Themeli, 2014, Morrison, 2014 cit in APAV, 2018).

HIGHLIGHT | INFORMATION IN FOCUS:

Empathy cannot, however, mean that the professional loses self-control and cries with the victim. Such conduct or reaction may cause, even if inadvertently, a negative impact on the victim and on the quality of the support process, as the victim may no longer understand the professional as someone qualified and prepared to provide support.

Some of the aspects that the professional should consider in the **empathic communication** are (APAV, 2019b):

- Maintain eye contact with the victim, on a calming, not inquisitive, way.
- Accompany eye contact with a serene and interested tone of voice and with body language showing availability and tranquility (for example, avoiding looking at the watch, showing any sign of impatience or performing unnecessary interruptions to the victim's speech).
- Use of interjections that reinforce and validate the victim's sharing of their cyber-victimisation experience and their courage in seeking support.
- Clearly demonstrate that you are listening carefully to the information the victim shares, including through nonverbal language (nodding yes, for example).
- Ensuring the victim that you understand the information they share, for example, by:

    - Reformulations – repeat in your own words the content transmitted by the victim. Rewording helps the professional to make sure they have understood properly the victim, but also indirectly assures/informs the victim that they are being listened to carefully, which will encourage them to continue.
    - Summaries - summarise the information shared by the victim, namely when closing a topic, at the end of a support session and/or at the beginning of the next one. Summarising can be

an excellent way to close information gaps and/or disagreements about what has actually been reported.

- Ensure the victim you are interested in and involved in the contact/interaction, by asking questions, for example. Aim for a balance between open and closed questions, which facilitates spontaneous communication and prevents the victim from feeling questioned. When approaching new subjects, and in order to promote the victim sharing information, choose open questions. Use closed-ended questions, on the other hand, to obtain concrete and specific information.
- Encourage emotional expression, especially when the person is in crisis. However, the professional should not impose emotional expression if the victim has not expressed their willingness to do so.

## 2.3. Information collection as a key step

Information gathering is a central process for supporting and intervening with any victim of crime, including victims of cybercrime.

The **first contact with the victim will be dedicated to this process of gathering information** on cybercrime, its impact and triggered needs. However, it is important to keep in mind that the **gathering and analysis of information are circular and constant steps**, which regularly feed into any process of support and intervention with victims of crime and cybercrime.

HIGHLIGHT | INFORMATION IN FOCUS:

It is not uncommon for the victim to show **signs of anxiety and discomfort in this first contact with the support professiona**l and/or the organisation providing support.

Professionals should consider that the victim may be, for the first time, sharing information about their cyber-victimisation situation, and it is normal that they show signs of discomfort, suffering and fragility, hesitation and/or shame. These indicators may be particularly prevalent when the information to be shared contains some kind of detail related to the relational and/or sexual intimacy of the victim.

The professional should (in line with the information summarised in Table 2):

- Respect the victim's silences, hesitations and pace.
- Strengthen the victim's courage in seeking support and sharing information about their history of cyber-victimisation.
- Explain and reassure the victim that their reactions, emotions/feelings and thoughts are normal, both in terms of discomfort at sharing information in a supportive context, and in terms of the experience of cyber-victimisation itself: in any case, these are natural reactions to unexpected or abnormal life events and circumstances.
- Demonstrate your willingness and availability to support and listen to the victim, including their fears, concerns and wishes.

# 2. KEY ASPECTS FOR CONTACTING WITH VICTIMS OF CYBERCRIME

The **collection of information should be adjusted to the victim's emotional state**, which means that, if the victim is not able to provide all the information, the professional should collect as much information as possible and, if this is not sufficient, subsequent care contacts should be scheduled in order to allow gathering more comprehensive information.

The victim's emotional well-being must be prioritised, even at the expense of the need to gather information.

In sum, collecting information from the cybercrime victim allows the support professional to:

1
- **obtain information about the cybercrime situation experienced by the victim**
- **assess the impact and consequences experienced by the victim of cybercrime**

2
- **asssess the risk of cybercrime (re)victimisation and victimisation in general**
- **set up cybersecurity measures and personal online protection behaviours**

3
- **identify the cybercrime victim's needs**
- **activate adequate resources and services to address the victim's needs and to address/minimise the impacts of the ciber-victimisation experience**

Figure II-1: Core areas/domains to be considered in the collection of information

The collection of information should be targeted at 3 areas:

1. **Personal and pre-victimisation history**
   The professional should seek to collect information on the family, professional and social context, and should also try to evaluate possible previous victimisation episodes, as well as Internet, ICT and social network usage habits, risk behaviour/activities, cybersecurity measures adopted or not, as well as personal online protection behaviours.

2. **Experience of cyber-victimisation**
   In this area, an attempt should be made to gather all possible information on the cybercrime situation experienced by the victim, with details of the circumstances, including: information on what happened; how it happened; which ICT and/or Internet-supported communication tools were used; with whom evidence of the cybercrime was disclosed/shared and/or through which platforms; who are the perpetrators and what is the relationship between the victim and the perpetrators; when did the cyber-victimisation situation start and whether it is ongoing; whether or not there is a co-occurence between cyber-victimisation and other forms of *traditional* victimisation involving the same perpetrators or others; what measures have already been taken by the victim.

3. **Post-victimisation history**
   The objective is to analyse and evaluate the impact of cyber-victimisation, understanding the consequences, the coping mechanisms put in place, the protective factors available to the victim, alongside evaluating the family and social support and the ability of the victim to manage the impact and regain control over their life. It is also be important to evaluate the victim's motivation for adopting preventive measures and setting up of a protection plan.

## 2.4. The specific case of children and young victims of cybercrime

As addressed in Part I of this Handbook[83], children and young people constitute a vulnerable group to cyber-victimisation due to their habits and behaviours in the use of the Internet and ICT, as well as by the adults' difficulty in supervising such behaviours (especially in the family context).

Contacting and supporting children and young victims of cybercrime should:

1. Always be guided by the **promotion and protection of their rights**;
1. Meet the characteristics and **stages of development** of the child or young person;
1. Contemplate, whenever possible, the **involvement of the family**;
2. To focus on educating for a safe and aware use of ICT and the Internet as a revitimisation protective behaviour.

Next, we examine in more detail each of these points.

**1**

- **promote and protect the children's rights throughout the support provided to a child/young adult victim of cybercrime**

When contacting and supporting children and young people who are victims of crime in general and of cybercrime in particular, professionals' actions should always safeguard the rights of children and young people. This Handbook does not intend to examine this matter comprehensively and, taking into account the particularities of the national legislation of each Member State, we may, in general terms, say that each professional who contacts with or supports a child or young victim should know the current legislation[84] and define their action accordingly.

The Convention on the Rights of the Child[85], which includes a set of basic universal rights to which all

[83] See Part I, section 3.2 of this Handbook.

[84] In the Portuguese case, Law no. 147/99, of September 1, on the Protection of Children and Young People in Danger and subsequent amendments, aims to promote the rights and protection of children and young people in danger, in order to ensure their welfare and full development. See legislation available at https://apav.pt/apav_v3/images/pdf/proteccao_criancas_jovens_perigo.pdf

[85] See full text at https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

children should have access, contains some fundamental principles that are suitable for any intervention with children and young people. They are:

- **The child's best interests**, which briefly states that all laws and actions affecting children should put the child's interests first, benefiting them in the best possible way.
- **Non-discrimination**, the principle that no child should be disadvantaged (or benefited) because of race, colour, sex, language, religion, nationality, ethnic or social origin, political or other opinion, economic status or physical or mental condition.
- **Survival, development and protection**, according to which the authorities should protect all children and help to ensure their full physical, social, spiritual and moral development.
- **Participation**, according to which all children have the right to have a say in decisions that affect them, as well as to be heard on matters that concern them.

Therefore, the professional and their support organisation should establish, define and implement their intervention in accordance with these principles and the relevant legislation, always bearing in mind the need to promote the **full exercise of the rights of children and young people**.

**2**

- **respect and take into account the child or young person's developmet stages during the support process**

Contacting and providing support to a child or young person victim of cybercrime must necessarily be distinct from that provided to an adult victim of cybercrime.

Professionals should know the main milestones in the **developmental process of the children or young person**, particularly on language and communication and adjust their communication strategies accordingly during the course of their work (APAV, 2019).

The following table summarises, in generic terms, the main milestones in the overall development process of a child or young person, according to age group.

**Table II-4: Key stages in a child/young person's development process**

| | Physical development | Emotional and cognitive development (including language) | Social and moral development |
|---|---|---|---|
| **3-6 years** | • Can draw and do other manual activities<br>• Can write their own name<br>• The body develops, taking the forms of the adult body<br>• Dexterity and coordination skills increase | • Recalls familiar experiences<br>• Uses some vocabulary<br>• Can adjust speech according to the interlocutor's characteristics (such as age, gender and social status) | • Can interpret, predict and influence other people's reactions<br>• Establishes the first friendships<br>• Self-aware emotions arise (such as shame and guilt)<br>• Has relative control over own emotions |
| **6-12 years** | • Progressive increase in weight and height<br>• Handwriting becomes smaller and more readable<br>• Drawings are more structured<br>• Games and jokes involving running, excitement and competition are commonplace<br>• Rapid response capability is developed at the level of motor dexterity<br>• Puberty indicators may be evident, particularly in the case of girls | • Thoughts and attention span are more focused<br>• Inductive reasoning<br>• Can relate experiences to specific occurrences<br>• Increase in vocabulary | • Becomes more independent and more responsible<br>• Distinguishes between being successful and unsuccessful<br>• Is aware of own efforts vs chance/luck in obtaining a given result<br>• Can put oneself in the other's place (empathy) |
| **12-18 years** | • Puberty<br>• Menstruation and fat tissue increase for girls<br>• Voice changes and there is an increase in muscle mass, in the case of boys<br>• Greater interest in sexuality | • Can discuss effectively<br>• More self-conscious and focused<br>• Development of hypothetical--deductive reasoning<br>• Can make subtle adjustments in speech<br>• Can make plans and take decisions | • Increasing conflict with parents/ family<br>• Closeness to peer groups and emergence of peer pressure situations<br>• Search for one's own identity<br>• Development of intimate relationships |

The following table presents some of the main differences in approach and communication with children and young people of different age groups to be taken into account by the professional in their contact and support process (APAV, 2011).

**Table II-5: Approach and communication with children and young people of different age groups**

| | 1-6 years | 6-12 years | 12-18 years |
|---|---|---|---|
| **Introducing oneself** | Fundamentally directed at the child.<br><br>The child is still too young to understand the information provided. | The child shows more interest in the information provided and greater ability to understand it. | The child/young person understands the information provided but may show reluctance to participate in an intervention programme or victim support process. |
| **Describing the event** | Expressed preferably through drawings or games, rather than verbal expression. | Able to communicate more details than younger children.<br><br>Older children prefer to express themselves verbally, sometimes refusing to use drawings and games. | The description of the event is detailed.<br><br>There are feelings of self-guilt. |
| **Psychoeducation** | Fundamentally directed at family/parents.<br><br>The child will assimilate simple information, such as acknowledging the situation, and they can simulate a way of dealing with it. | Aimed at the child, integrating the family/parents in the psychoeducation process. | Directed to/through the child. |

In addition, it is important that professionals, when contacting or supporting the children or young people victims of cybercrime, create all the conditions, namely through the **way they communicate with the children/young people**, to prevent them from experiencing the situation as a kind of 'police interrogation'. This is definitely not the intention and it is important to have a comfortable and informal environment, contributing towards the establishment of a trusting relationship between professionals and the children/young people victims.

With younger children, the support may require the presence of a relative or legal representative until the child gets used to the professional and feels safe without the relative or legal representative (APAV, 2019).

- **Involve the family whenever possible**

**3**

The **role of the family and parents** is crucial in situations of cybercrime targetting children and young people. They have a preventive role, by informing, supervising and, where appropriate, restricting the use of the Internet and ICT by children and young people (Öztürk & Akcan, 2016). The **involvement of the family in situations where cybercrime has already taken place is equally important** since:

- they have an important role in informing about the child or young person's life story;
- the participation/frequency of the child or young victim's engagement in the support process depends to a large extent on the family/parents' availability and willingness;
- they are also key elements for the psychoeducation of children or young people and the prevention of revictimisation.

Professionals should understand to what extent becoming aware of the children/young people's cyber-victimisation experience contributed to changes in the personal, marital and family functioning. **Addressing the impact and consequences of the cyber-victimisation experience on the family will also contribute to the recovery of the child**. The family's reactions to the experience of cyber-victimisation of children and young people are in all respects similar to the reactions to situations of *traditional* violence and crime (APAV, 2011):

- **Desire for revenge**. A common reaction, associated with a feeling of revolt, is the desire for revenge, to take 'justice into their own hands';
- **Feeling guilty**. The family may feel guilty for not having discovered/suspected that the child or young person was being subjected to crime or violence;
- **'Tough subject'**. Talking to the child or young person about the violence they have been a victim of is usually a very difficult challenge for the family and parents. Even so, this dialogue is important to establish greater trust in the relationship between the family and the child or young person. However, the family may also try to put pressure on the child or young person to talk about the victimisation situation, which may prove counterproductive;
- **Relational change**. The relationship with the child or young person can also change: the *family/parent-child/young people victim* relationship can become more difficult and clouded by embarrassment and reciprocal feelings of guilt and shame;
- **Distrusting the intervention**. In many cases, the family may express a lack of trust in the institutions, particularly police authorities. The fact that they are not provided with information on ongoing investigations is a key factor;
- **General impact on life**. All areas of personal, family, social and professional life of family members and parents may be affected;
- **Need for support**. In addition to the support and work with the children or young people who are victims of cybercrime, the family and parents may also need specific support to help them as much as possible in the tasks and challenges indicated above.

# 2. KEY ASPECTS FOR CONTACTING WITH VICTIMS OF CYBERCRIME

The professional and their organisation's actions in situations of cyber-victimisation of children and young people should also be concerned, in addition to responding to the needs arising by the experience of cybercrime, with the **promotion of safe and conscious behaviours when using the Internet and ICT** – the aim is to prevent the involvement of children or young people in new risk situations or situations of repeated cyber-victimisation.

It is important to ensure that children and young victims are educated in the safe and appropriate use of the Internet and ICT, which includes, for example: adopting appropriate online behaviours for personal protection; the positive and safe use of ICT and the Internet; implementing cybersecurity mechanisms in ICT and communication tools supported by the Internet; identifying situations of risk of cyber-victimisation and acting adequately (Martellozzo & Jane, 2017; Wolak, Finkelhor, Mitchell & Ybarra, 2010; Lwin, Ang & Liu, 2013; Wright, 2015).

HIGHLIGHT | PRACTICES IN FOCUS:

In the UK, the *ThinkUKnow* programme provides information tailored to children of different ages, as well as families, parents, legal guardians and educators about cybercrime and online safety.

This programme, created by the *Child Exploitation and Online Protection Centre* (CEOP), provides safety advice and information on a range of issues related to the use of the Internet and ICT and the resulting risk situations (Marczak &Coyne, 2010).

The platform is available at: www.thinkuknow.co.uk/

# 3. PROVIDING SUPPORT TO VICTIMS OF CYBERCRIME

In this chapter of the Handbook, and in close connection with the overall guidelines for contact, communication and information gathering discussed in the previous chapter, we will focus on support and intervention for victims of cybercrime.

Keeping in mind the consequences of the cyber-victimisation experience and the needs for support that have been examined in Chapter 4 of Part I of this Handbook, we will focus on emotional support, crisis intervention and the central aspects of expert support for cybercrime victims.

Considering the wide range of cybercrime forms, it is important to stress that the content presented here is not considered the only possible response to be implemented with any victim of cybercrime. On the contrary, it constitutes a wide-ranging roadmap, contemplating guidelines for action that may help professionals and organisations adjust the set up and delivery of their interventions in terms of their own characteristics and objectives and aiming at providing the best possible response to the needs of victims of cybercrime

HIGHLIGHT | INFORMATION IN FOCUS:

As this chapter and previous ones of the *Intervention* part of this Handbook assume that support for victims of cybercrime is provided by organisations, namely victim support organisations, some **basic requirements and practical aspects for the development and operation of support services for victims of cybercrime** need to be addressed.

Any organisation intending to develop and implement a support service or response aimed at victims of cybercrime should primarily consider conducting a **diagnostic assessment of its organizational capabilities**[86].

Some of the areas that the organisation should analyse internally are:

- Adequacy of this service or support response to the mission and activities of the organisation itself and, when applicable, levels of integration with their other services (such as services and support responses for victims of crime and violence);
- Financial capacity to leverage the development of the support service or response and its operation, considering in particular the existence or not of own resources, access to external financing and/or sponsorship;
- Access to material, technological and logistical resources necessary to develop and operate the service or support response;
- Organisational knowledge about the support to be provided and about cybercrime, including the different types of cybercrime, the risk factors and the impact of cyber-victimisation and the applicable legal framework;
- Organisational technical capacity to develop procedures for the service or support response that it intends to operate, considering its suitability in light of the mission, principles and values of the organisation, the other forms of support/services it provides and applicable legislation;
- Current (formal/informal) partnerships with other organisations with experience and expertise in this field and possibility of participation/development of actions enabling sharing/obtaining knowledge, experiences and good practices;
- Existing human resources (remunerated and/or volunteers) qualified to provide this type of support and technical and financial capacity for their preparation and qualification.

[86] Adapted from Safety Net Project - https://www.techsafety.org/resources-agencyuse.

# 3. PROVIDING SUPPORT TO VICTIMS OF CYBERCRIME

Thus, in summary, **the organisation's preparation for implementing** a response or support service for victims of cybercrime will include the following basic steps:

1. Define the objectives of the intended response or support service. Some of the objectives may be, for example: information/awareness; emotional support; practical support; more specific support or advice at a certain level (e.g. legal information); referral to other services/responses/organisations fit for dealing with the situation.
2. Identify the recipients of the response or support service: the purpose may be implementing a response or support service and/or information to victims of any form of cybercrime; or it may be target specific groups of victims and/or specific forms of cybercrime. An example is the reporting pathways for child sexual abuse or exploitation material.
3. Establish procedures and strategies for articulation and integration with the other organisation's responses and support services for victims of crime, if available, defining how and in what way information on a particular situation of cyber-victimisation will be dealt with internally, if necessary, for best addressing to the victim's needs. External links and interinstitutional cooperation should also be considered[87].
4. Develop specific procedures for the support to be provided, considering the objectives and recipients of the response or support service and the applicable legislation[88] and professional codes of conduct, when applicable. In addition, the organisation should also have a broad understanding of the phenomenon, its impact on victims and the needs triggered by experiences of cyber-victimisation[89].
5. Select and train human resources for the operation of the response or support service[90].
6. Disseminate and advertise the response or support service[91].

## 3.1. From emotional support to crisis intervention

Succintly, the emotional support to a cybercrime victim is largely based on the professional's positioning and attitude concerning the dimensions already discussed in this Handbook and listed below:

- **Empathic communication**, which includes active listening;
- **Non-verbal language** demonstrating availability, openness and consistent with active listening;
- **Acknowledging the complaint** and **respect for the victim's pace** when sharing;
- Promoting the **victim's emotional expression and validation** of their experience, reactions, emotions/feelings, behaviours, thoughts and meanings attributed to that experience.

In that context, we stress again that **this emotional support is especially important when gathering information** from the crime victim about their experience of cyber-victimisation (not least because gathering information, with the subsequent need to share information about the experience of cyber-victimisation, can trigger negative memories and feelings about the experience of cybercrime; moreover, gathering information is in itself an uncomfortable and vulnerable moment for the victim). Therefore, this emotional support remains important throughout the intervention with the cybercrime victim, regardless of the shorter or longer length of the intervention.

[87] See sections 3.5.1.3. and 3.5.3.2. of Chapter 3 of Part II of this Handbook for further information on working collaboratively.

[88] See Part I, Chapter 2 of this Handbook for detailed information on the legal framework on cybercrime.

[89] See Chapters 1, 3 and 4 of Part I of this Handbook for comprehensive information on the phenomenon of cybercrime, explanatory theories, risk factors associated with cybercrime and its impact.

[90] See Part II, Chapter 1 of this Handbook for information on the professional's personal and technical skills for supporting cybercrime victims.

[91] See Part II, section 4.2 of this Handbook for information on the role of public information and awareness campaigns in disseminating information on existing resources for supporting and protecting victims of cybercrime.

However, in certain circumstances, the victim of cybercrime may seek the support of the professional and their organisation (namely victim support organisations) in a **crisis situation**.

HIGHLIGHT | INFORMATION IN FOCUS:

The experience of cyber-victimisation, by its potentially unusual and unforeseen character and the (real or perceived) threat to the physical and/or psychological integrity of the victim, can potentially lead to a **crisis situation** (APAV, 2013).

The crisis situation is observable through the following manifestations:

- **Intense psychological reactions**, such as crying, panic, confusion, anguish, shame, low self-esteem, guilt, anger, psychosomatic disorders[92] and predominance of memories about the event;
- **Social and economic pressures** that lead to emotional or psychological blockage, associated with n**ot knowing their rights**.

The duration and intensity of the crisis situation depends on the degree of violence against the victim, their internal resources to deal with the problem and the external resources at their disposal, including support (informal and formal) received after the victimisation situation.

Crisis intervention (or psychological first aid) is therefore an intensive, focused and time-limited action, oriented towards solving current problems and responding to specific objectives. It is a response providing initial support and practical, non-invasive care, in crisis or emergency situations.

The initial task of the professional who contacts with a victim of cybercrime in a crisis situation is therefore related to:

- **Assessing the victim's safety** and **self-care capacity** in potentially traumatic situations, considering that the personal and social resources available to them may be insufficient to respond adequately to a highly demanding situation.
- Operationalisation of intervention tasks aimed at the **recovery and reorganisation of the victim**, reducing the negative impact of cyber-victimisation and ensuring their safety and physical and psychological well-being.

Crisis intervention should seek to respond to the following objectives, similar to the general guidelines for supporting victims of cybercrime (see Table 2):

- Break with the idea of 'unique vulnerability';
- Deal with the search for explanations;
- Deal with the victim's feelings of guilt;

[92] Psychosomatic disorders are related to the physical presentation (e.g. nausea and stomach pain) of psychological problems and disorders.

- Avoid silencing or pressure 'to forget';
- Promote hope in the recovery and resolution of the problem;
- Explain the necessary legal procedures.

Crisis intervention should therefore be based on the following **steps**:

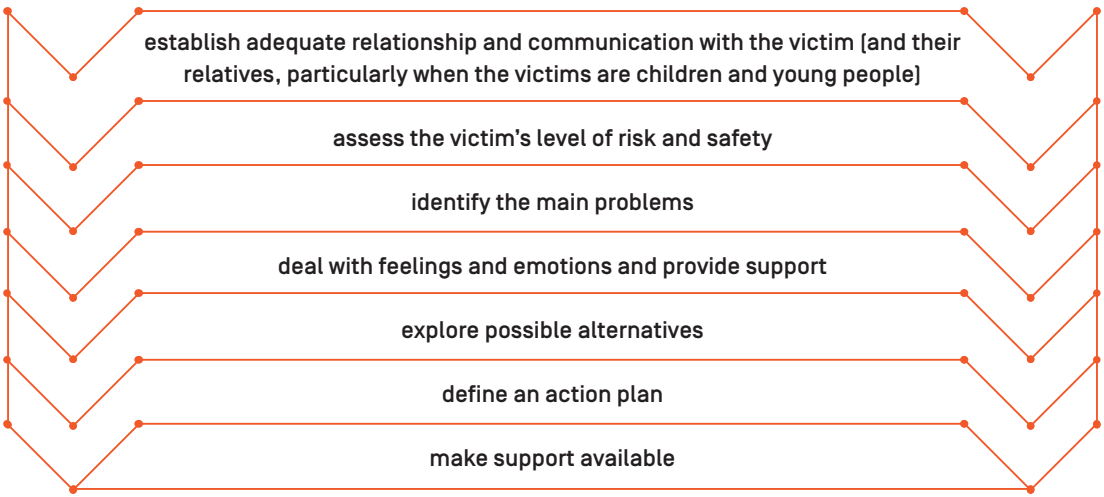


Figure II-2: Steps to be followed during a crisis intervention

In this type of intervention, we suggested adopting the following strategies, without prejudice to others that may be deemed appropriate (APAV, 2013):

**Establish a rapport with the victim:**
The professional should try to establish a relationship of trust with the victim, identifying the events that led to seeking support, which will allow identifying the key problems.

**Assess:**
Professionals should be aware of the victim's mental health, whether there are suicidal thoughts, how much anxiety, agitation and distress they are experiencing and, in particular, whether their mental situation allows them to adequately respond to the practical obligations arising from cyber-victimisation.

The professional should also assess the risk (further details will be covered in the following sections of this Handbook), as well as the existence and quality of the support provided by the primary support network (family and/or friends).

**Reduce stress and anguish:**
It is common for the victim to find themselves in a situation of stress and anguish. Communicating with the victim in a safe and reassuring manner is an appropriate strategy to reduce these symptoms. Similarly, when contacting the victim, the professional should explain that these reactions are normal, legitimate and may occur in the face of negative, challenging and/or demanding personal experiences.

In this process, the professional should communicate naturally with the victim (without neglecting the seriousness of the situation experienced), paying attention to them and not reinforcing agitated or emotionally distressed behavior.

**Show interest and motivate the victim:**
The professional should show interest, willingness to listen and understand the victim and their situation (see section 2.2 on empathy in this part of the Handbook). They should also stimulate hope in a positive (though realistic) resolution of the situation, which will promote the victim's self-confidence.

It is also important to encourage the victim to find their own strategies to overcome the experience of cyber-victimisation by strengthening their capacities.

**Clarify:**
It is important to clarify what requirements the victim will have to address as a result of the cybercrime suffered, including practical obligations such as liaising with banks in financially motivated cybercrime situations, for example, or liaising with platforms where illegal content is available to request its removal.

**Inform and validate the rights of the victim:**
The professional should provide the victim with information on their rights, on the functioning of the justice system and on the advantages and disadvantages of reporting the crime, thus contributing to an informed decision by the victim on this matter. One of the advantages that may be associated with the decision to report may be the victim's reassurance that they have taken an active attitude towards the crime they suffered. Another advantage that the professional can highlight is that, by reporting their specific situation, the victim is contributing to prevention and enabling other people to be 'spared' from experiencing similar cyber-victimisation situations. The disadvantages are related to the difficulties that the victim may face throughout the judicial process, namely possible obstacles in the criminal investigation and their own emotional difficulties, such as shame and the need to relive the traumatic event each time they are asked to report the facts.

The professional should alert the victim to the need to preserve the evidence of the crime if they have access to them (such as, for example, links where it is possible to access information on the acts of aggression online to which they have been subjected, as well as messages, videos and/or other files they have received during the cyber-victimisation or even prints/copies that account for the online advertising/dissemination of the aggression).

**Referral to judicial and police authorities:**
If the victim has not yet contacted the judicial and police authorities for the investigation of these crimes by the time they contact the support professional, then the professional can, with the victim's consent, facilitate such referral. For this purpose, it is important that the professional's organisation defines and/or seeks to implement mechanisms to facilitate interinstitutional cooperation, which we will also address in this Handbook (see sections 3.5.1.3. and 3.5.3.2. in this chapter, Part II of this Handbook).

**Provide support:**
The professional should make available to the victim the support services and responses available via their organisation, which may include, for example, referral to more specific support services provided by their organisation and even external resources available, at local, regional or national level, through interinstitutional articulation and cooperation.

HIGHLIGHT | PRACTICES IN FOCUS:

APAV coordinates, in Portugal, a specialised network in the support to children and young victims of sexual violence, called CARE Network, which provides psychological, social and legal support to children and young victims of sexual violence, but also to relatives and friends.

This Network has specialized professionals, distributed across the national territory, seeking to ensure a decentralised quality service. By providing itinerant services, CARE Network's victim support specialists guarantee children and young victims, their families and friends access to multidisciplinary support, adjusted to their identified needs and near their respective areas of residence.

Thus, when a situation of sexual violence against children and young people is identified in any APAV support service - such as a Victim Support Office or the Integrated Distance Support System / Victim Support Line | 116 006 -, there is a (internal) referral of the case to specialized support by the CARE Network.

Additional information on the operation of APAV's CARE Network is available at www.apav.pt/care.

Following crisis intervention, it may be necessary to continue the intervention with the victim of cybercrime to promote their recovery and respond appropriately to their needs. In line with the support responses provided by other victim support organisations to other forms of victimisation, this Handbook will also address the central aspects associated with specialised legal, psychological and social intervention, and these areas will also be in line with the needs usually identified by victims of crime. The key aspects of specialised intervention will be discussed in section 3.5 of this chapter.

## 3.2. Assessing the risk of revictimisation

The assessment of the degree of risk of revitimisation evaluates the **likelihood of new cyber-victimisation against the victim**. After gathering information (see Chapter 2 of this part of the Handbook), the professional should assess the victim's risk and protection factors evidenced during intervention, so that the needs for support and intervention can be identified.

The process of assessing the risk of revitimisation thus results from the convergence between the **information shared by the victim** regarding their experience of cyber-victimisation and the use of that information to **identify (in a more or less structured way) the revictimisation risk factors** (and which will be given particular attention in planning the intervention, and personal online protection behaviours and cyber-security measures in order to prevent revitimisation). The **supporting professional's experience and judgment** is also important in this risk assessment process.


Figure II-3: Assessment of the risk of revictimisation

As mentioned in Chapter 3 of Part I of this Handbook, the research on risk factors associated with cyber-victimisation is not, to date, especially extensive, and although other factors or variables may still be identified, **individual factors related to the victim's behaviour**, particularly the intensity and habits of use of the Internet and ICT and the type of activities carried out online, have been associated with increased vulnerability to cybercrime and the risk of cyber-victimisation (Wilsem, 2013; Brown et al., 2017; van der Wagen & Pieters, 2018). On the other hand, the multiplicity of cybercrime forms also makes it difficult to identify a group of risk factors or variables that are unequivocally applicable to any type of cybercrime.

[93] For additional information on risk factors associated with cyberbullying, please refer to Part I, Chapter 3 of this Handbook.

Even so, if only in general terms, we can say that the assessment of the risk of revitimisation should focus on **three risk areas**:


Figure II-4: Assessment of the risk of revictimisation – areas/domains

However, and alluding again to the multiple nature of cybercrime, it is clear that, for example, the **analysis of the revictimisation risk from cybercrimes against computers and computer systems** (cyber-dependant crime)[94] has difficulty collecting information that allows this tripartite reading of risk (based on the victim's characteristics, the cybercrime dynamics and the perpetrator's characteristics). As an example, in these cases the perpetrator acts anonymously, and it is very difficult to identify their real identity, so the analysis of their characteristics and their contribution to the increase/reduction of the revictimisation risk is, therefore, negatively affected.

On the other hand, the identification and analysis of risk at three levels is be more useful in determining the victim's vulnerability to **revictimisation in cases of cybercrime facilitated or practised through computers and information systems**[95], particularly in situations where there is a relational link (online and/or offline) between victim and perpetrator, as these cases more easily correspond to a transposition of *traditional* crime into cyberspace.

The following table presents some variables and risk factors associated with each of the above risk areas, which can be used by the professional to assess the victim's risk of revictimisation.

However, one should keep in mind that these are indicative and generic variables and do not consider the specific dynamics associated with each particular situation of cyber-victimisation.

[94] See Part I, Chapter 1 of this Handbook for detailed information on this conceptualisation.

[95] Ditto.

**Table II-6: Proposed variables for assessing the cybercrime victim's revictimisation risk**

| Characteristics of the victim | Characteristics of cybercrime |
|---|---|
| *Risk factors relating to the victim's socio-demographic and individual characteristics and risk factors associated with Internet and ICT usage behaviour.* | *Characteristics and dynamics of cybercrime, including the [online and/or offline] relationship/connection between victim and perpetrator, particularly in situations of cybercrime facilitated by the Internet and ICT.* |
| **Age**<br>*Differentiated levels of risk of cyber-victimisation have been evidenced in children/young people and in elderly people; in the former, by habits of intensive use of Internet and ICT and, in the latter, by the lack of technological literacy.*<br><br>**Gender**<br>*There is no agreed view from research and prevalence studies and this variable should be interpreted with caution. Although the female gender is associated with higher levels of victimisation across different cybercrimes, this may be due to greater reporting. In some cybercrimes, males are also associated with more severe and serious forms of aggression.*<br><br>**Other individual variables associated with greater vulnerability to victimisation**<br><br>Presence of mental and/or cognitive difficulties/disability<br>*These characteristics may limit or hinder the identification/recognition of cyber-victimisation and/or the disclosure/request for support following cyber-victimisation, which increases the risk of re-victimisation.*<br><br>Primary language<br>*In situations where the victim's primary language is different from the language in which cybercrime support/reporting can take place, the risk of revictimisation is greater and associated with greater vulnerability to social exclusion and isolation.*<br><br>Previous victimisation experiences<br>*If the victim has already been the target of cybercrime in the past, the re-victimation risk may be higher, particularly if the factors of exposure to cybercrime have not changed.*<br><br>No informal support [e.g. family; friends; co-workers]<br>*Social isolation, particularly the absence of closer and more significant social relations, is a risk factor for victimisation.*<br><br>**Risk factors associated with Internet and ICT usage behaviour**<br><br>Technological literacy<br>*Internet and ICT skills and knowledge seem to reduce the risk of cyber-victimisation. Their absence/insufficiency, on the other hand, seems to increase this risk.* | **Knowing the cybercrime perpetrator**<br>*The risk of re-victimisation is greater in situations where the perpetrator and victim know each other [online and/or offline). In these cases, knowledge of the victim's daily routines, both online and offline, is greater, which increases the risk of revitimisation*<br><br>**Relationship with the cybercrime perpetrator**<br>*In situations where victim and perpetrator have had some kind of offline relationship [such as former intimate partners, co-workers, friends], the risk of re-victimisation is higher.*<br><br>**Existence of a history of victimisation by the cybercrime perpetrator**<br>*The existence of previous victimisation experiences practiced by the same perpetrator indicates a risk of revictimisation. One of the best predictors of the perpetrator's current behavior is their past behaviour.*<br><br>**Severity and impact of cybercrime**<br>*For example, the fact that cybercrime may have triggered symptoms of emotional and psychological distress [such as panic attacks, intense fear, flashbacks, nightmares, profound sadness, or other symptoms/signs], may reduce the ability to seek support in current/future victimisation situations.*<br><br>**Duration and escalation of cybercrime**<br>*If cyber-victimisation persists - as it occurs in many cyberstalking situations, for example - in addition to the likelihood that the illicit conduct becomes more intrusive and aggressive for the victim, it also reinforces the perpetrator's behaviour, increasing the risk for the victim.*<br><br>**Being afraid of the cybercrime perpetrator**<br>*The victim's perception of fear towards the perpetrator, particularly in cases where they know each other, is a very important indicator, even though there are situations where the risk is underestimated.*<br><br>**Previous [unsuccessful] attempts to solve the situation**<br>*In addition to the victim's discouragement, this failure encourages the perpetrator to practice new acts against the victim, increasing the risk.*<br><br>**Reporting/complaining**<br>*Reporting is a moment of risk for the victim, given the possibility of retaliation/revenge by the perpetrator.* |

**Internet and ICT usage levels**
*People with higher levels of Internet and ICT usage (e.g. daily) have a higher risk of cyber-victimisation.*

**Type of activities performed online/content usually consumed**
*Higher rates of disinhibition in online behaviours and interactions, as well as more unsafe behaviours (such as downloading files of unknown origin) are associated with increased vulnerability to cyber-victimisation.*

**Characteristics of the perpetrator of cybercrime**

*Personal and social characteristics of the perpetrator of cybercrime, their previous conduct and other indicators of danger which can indicate a higher risk of revictimisation for the victim, particularly in situations of cybercrime made possible or facilitated by the Internet and ICT.*

NOTE: In this risk analysis, in addition to the difficulties associated with cybercrime typologies mentioned above, the information shared by the victim may not be sufficient to assess the factors presented below.

Existence of **mental health problems and/or drug use** by the perpetrator of the cybercrime (known by the victim)

Existance/history of **problems with the justice system** by the perpetrator of the cybercrime (known by the victim)

Attempts to **contact/approach/intimidate** the victim after the episode that motivated the victim to seek support

The perpetrator's desire for revenge, particularly when victim and perpetrator had a previous intimate relationship and cybercrime arises as a form of retaliation for endind the relationship (for example, non-consensual disclosure of images and videos)

Particular interest in cybercrime, e.g. financial motives and/or sensation-seeking

## HIGHLIGHT | INFORMATION IN FOCUS:

The professional (and the organisation where they work) should decide and define how to conduct the collection of information for assessing the risk of re-victimisation. In general:

- The collection of information can be carried out indirectly by the professional, using the information shared by the victim when contacting the organisation/professional;
- The assessment of the risk of re-victimisation can be carried out in a more structured manner, asking concrete questions on each of the variables listed above (or others considered relevant) and/or through specific instruments.

It is also important to remember that **assessing the risk of revictimisation is useful only if it is accompanied by measures to help the victim managing and dealing with the situation and risk**, in order to improve their safety and prevent revictimisation.

When defining parameters and variables to assess the risk, the organisation and/or the professional should also consider developing an information and a protection plan for the victim, taking into account the risk

variables identified. The **protection plan** represents a set of strategies for the prevention of revictimisation, agreed and defined between victim and professional, which includes protection measures and behaviours against new crime situations, as well as strategies and practical instructions for dealing with and acting with another eventual reoccurrence of cybervictimisation.

The protection plan (Finn & Banach, 2000) can include, depending on the type of cybercrime the victim has suffered:

- Adopting cyber security measures and personal protection behaviours to prevent revictimisation, such as: storing important information in password-protected files and directories; encrypting most important data; avoiding logging in and/or sharing personal information in public or using open wi-fi networks; changing passwords; updating antivirus software; modifying privacy settings on social networks;
- Identifying signs of a risk of cyber-victimisation, for example: constant redirection to strange/unknown web pages; appearance of pop-up messages, images, strange sounds or applications installed without consent, etc;
- Practical information on how and where to get help in a victimisation situation.

## 3.3. Assessing and identifying support needs

Following the collection of information with the victim, and considering the results of the assessment of the risk of revictimisation, it is important that the professional identifies the support needs of the cybercrime victim.

Some aspects that can help the professional identify the needs to be addressed are:

- To what extent and in what way(s) does the victim feel that they have been affected by the crime/cybercrime targeting them?
- How is the experience of cyber-victimisation affecting the victim's psychological and emotional functioning and well-being?
- How is the experience of cyber-victimisation affecting the victim's physical health?
- How is the experience of cyber-victimisation affecting the victim's relational, work/occupational and social functioning?
- How is the experience of cyber-victimisation changing the victim's routine and quality of life (general well-being)?
- How is the experience of cyber-victimisation affecting personal perceptions of safety and cybersecurityy (including fear of crime)?

- To what extent has the experience of cyber-victimisation affected people in the victim's close social network and what are these impacts?
- What does the victim wish and need to happen after the cyber-victimisation experience?

Depending on the response to the previous questions, the professional, together with the victim, should find out whether:

- Is it necessary to provide strategies to increase the victim's safety to deal with possible new episodes of crime?
- Is it necessary to recommend that the victim contact the police/judicial authorities?
- Is there a need to make the victim aware of the need for more specific support, information and/or interventions (e.g. legal, medical, psychological or other)?
- It is necessary to motivate the victim of the need to be referred to other services or organisations (e.g. for specific medical/psychiatric support).

HIGHLIGHT | PRACTICES IN FOCUS:

As part of the EVVI Project (*EValuation of VIctims*), promoted by the French Ministry of Justice, an individual assessment questionnaire of victims' needs and a practical guide were developed.

This tool for assessing the needs of victims is structured in different areas:

- Individual characteristics of the victim and personal vulnerability such as age, gender, ethnicity, presence of physical and/or cognitive limitations or disabilities, among others;
- Risk and fear of crime, including the type and nature of the crime and its circumstances;
- Assessment of the victim's current situation;
- History of victimisation and information about the perpetrator.

The guide and the assessment tool are available at http://www.justice.gouv.fr/publication/evvi_guide_en.pdf.

Some of the **needs identified** can be met by the organisation supporting the victim of cybercrime, via its services and support responses.

However, other needs (e.g. medical and psychotherapeutic support) may require **inter-institutional cooperation and the involvement of other structures**, for example the criminal justice system and other systems. Moreover, inter-sectoral partnerships, including those between the state and civil society and voluntary organisations, appear to be important for better addressing the needs of victims of cybercrime, as they contribute to increasing the flexibility and accessibility of such services and support responses (Wedlock & Tapley, 2016).

HIGHLIGHT | INFORMATION IN FOCUS:

The organisation's capacity to respond to the needs of the victim of cybercrime will depend on:

- the organisation's competences and mission;
- the existence/availability of support services or responses provided by the organisation and to which the professional can refer the cybercrime victim for specific/specialized support;
- the existence of community support services or responses (e.g. Health, Social Security, Justice and Safety) and even possible protocols for interinstitutional cooperation[96].

## 3.4. The role of support via the Internet in supporting victims of cybercrime

Up to this point in this Handbook, we have been addressing contact and support with victims of cybercrime assuming that these take place through conventional (i.e. face-to-face and even telephone) modalities of support, information and intervention. However, just as crime and violence have been crossing physical and conventional barriers and have embodied the emergence of cybercrime and the multiple phenomena associated with it, contact and support for victims of crime have also evolved.

Internet support services provided by victim support organisations for supporting and informing victims of crime are becoming increasingly common.

Similarly, support for victims of cybercrime can also be provided through conventional support services (including face-to-face support and telephone support), as well as through Internet support services, the latter considered as equally valid channels for access to a wide variety of services (Dooley et al., 2010).

It is therefore important to deconstruct some aspects associated with support via the Internet.

**Internet support** is a comprehensive designation that refers to all support, information and/or intervention obtained remotely through the Internet and ICT (Mallen, Vogel, Rochlen, & Day, 2005, Barak, Klein, & Proudfoot, 2009 cit in APAV, 2017).

This designation covers a diverse set of methods, including intervention or support mechanisms where there may or not be interaction between a user and a professional. The different methods of support through the Internet may differ in the (in)existence of interaction with a professional, but also in the vehicle used to communicate (e.g. audio, video and/or text), how they complement other forms of intervention/support and how the communication is conducted (synchronous or non-synchronous) (Robinson, 2009, Callahan & Inckle, 2012 cit *in idem*).

[96] See points 3.5.1.3. and 3.5.3.2. of this Chapter of Part II of the Manual for information on interinstitutional cooperation and networking.

# 3. PROVIDING SUPPORT TO VICTIMS OF CYBERCRIME

There are multiple forms of Internet support, namely: Internet-based intervention/support programs; online support; blogs, online forums and mutual help groups; Internet-operated software; other self-administered forms of online support (Barak et al., 2009, Dowling, & Rickwood, 2013 *cit in idem*).

Among the different forms of support via the Internet, **online support** stands out as the remote support approach that most closely resembles traditional support responses, information and/or face-to-face intervention.

Online support pertains to the provision of support and/or information to a victim of crime in which (APAV,2019):

- Communication is conductedt using the Internet and ICT;
- Support and/or information is provided remotely (i.e. at a distance), where the professional and the victim are in different physical spaces;
- Communication can be conducted synchronously (in real time, as is the case of chat services and communication through applications such as *Skype*® or *Whatsapp*®) or asynchronously (where there is a time gap between the communication by the victim and the professional's response, as is the case of e-mail messages or online forms).

Despite the sparse evidence on the effectiveness of Internet and online support, particularly in interventions with victims of crime, several advantages and benefits have been pointed out.

HIGHLIGHT | STATISTICS IN FOCUS:

Under the *T@LK Project - online support for victims of crime*, financed by the European Union Justice Programme, a survey on distance support and online support for victims of crime was conducted with 60 organisations and victim support services in Europe. Among other topics, this survey explored the advantages of providing online support to victims of crime:

- 82% of the participating organisations mentioned *accessibility* to support services as an advantage.
- About 80% of the participating organisations with online support indicated *convenience* and *flexibility* in accessing support services as advantages, with a smaller proportion (58%) without online support services to victims of crime indicating convenience and flexibility as positive aspects.
- *Facilitated access*, particularly for victims with difficulties in accessing conventional support services, was indicated as an advantage by 60% of the participating organisations with online support services for victims of crime and by 74% of the participating organisations without online support services.
- *Facilitating a victim's first contact with support services and organizations* was indicated as an advantage by 71% of those with online support, but by only 42% of those without online services to support victims of crime.
- A *greater number of victims who can access support* was indicated as an advantage by 79% of the participating organisations without online support services, but on a smaller scale (57%) by organisations with online support services for victims of crime.

O relatório completo com informação detalhada sobre este e outros resultados do inquérito está disponível em: https://www.apav.pt/publiproj/images/yootheme/PDF/TALK.pdf.

HIGHLIGHT | PRACTICES IN FOCUS:

Under the same project, *T@LK Handbook - online support for victims of crime* was developed. It is a handbook for victim support organisations, helping them to understand support via the Internet, as well as to create and/or implement online support services for victims of crime.

It can be accessed at https://www.apav.pt/publiproj/images/yootheme/PDF/Handbook_TALK.pdf

## 3.5. Specialised support for victims of cybercrime

Following the intervention, particularly a crisis intervention, and taking into account the information provided by the cybercrime victim and the support and protection needs identified, it may be necessary to refer (internally or externally) the cybercrime victim to specialised support responses, particularly at legal, psychological and social level, in order to minimise the cybercrime consequences, to reorganise the victim's life and to address their needs.

### 3.5.1. Legal support: objectives and key aspects

Legal support to victims of cybercrime should be provided exclusively by law professionals, but it is very useful that any support professional be aware of the national legal framework and other Community and international legal instruments on the applicable legal regime. For this purpose, it is recommended reading and consulting Chapter 2 of Part I of this Handbook, which covers the legal framework of cybercrime.

It is also essential that the support professional is aware of the various stages of the criminal procedures and the extent to which they can inform and support the victim at each stage and on their rights as a victim of crime.

Legal support comprises information and tasks that enable the professional to accompany and support the victim of a crime before, during and after the various stages of the criminal process.

The legal support consists of:

- Information on the types of cybercrime and their legal framework;
- Information and advice on the rights of victims of crime;
- Support in the analysis of court notifications and drafting responses;
- Support drafting a claim for reimbursement of expenses incurred as a result of participation in the proceedings;

- Support drafting a request to explain their absence from judicial acts;
- Support writing and submitting a complaint/report;
- Support/accompaniment by the support professional when presenting a complaint/report;
- Support in writing and filing a civil claim (when the victim can present it, rather than a lawyer);
- Support in writing requests for the application of protective measures.

#### 3.5.1.1. The rights of victims of crime

A key starting point when supporting the victim of a crime is to ensure that, at any stage of the criminal process, the victim has **effective access** and **exercises their rights in an informed manner**.

The transposition into national law of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012, which establishes minimum standards concerning the rights, support and protection of victims of crime, seeks to strengthen the position of victims and their individual needs for support and protection in their journey through the criminal justice system, emphasizing the duty of States to protect victims of crime, their relatives and friends from secondary or repeated victimisation, intimidation and/or retaliation. This Directive also reinforces the essential role of victim support organizations, either in their complementary role, or as a substitute for the State, in ensuring access to qualified, free and confidential support services, or as a catalyst for the effective and informed exercise of rights by victims of crime.

This Handbook does not replace reading the Directive in its entirety[97], and it stresses the importance of having a complete knowledge of the various rights covered by this instrument.

Below, we present a summary of some of these rights, and highlight, once again, the importance of reading this legal instrument, as well as consulting information on the practical implementation of these rights at http://www.infovictims.com/com/.

***Right to information***

The right to information is fundamental as it enables the crime victim to participate in an informed manner in the criminal proceedings and to exercise their rights. Crime victims have the right to receive information on their rights, in particular, when they first come into contact with security forces or judicial authorities:

- what type of support they can get and who can provide it;
- how and where to report or complain about a crime;
- how and under what circumstances they may require protection measures;
- how you can they obtain legal advice or legal aid;
- how and under what circumstances they can claim compensation from the offender;
- how and under what circumstances they can claim compensation from the State;

[97] The complete document is available at: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX-%3A32012L0029 .

- If the victim does not speak the language used in the criminal proceedings or has a disability, how can they receive interpretation and translation services;
- if they do not reside in the Member State where the crime occurred, what procedures are in place for them to exercise their rights in that country;
- if the authorities do not respect the rights of the victim, where can the victim go to make a complaint;
- which contacts they should use to obtain or add information about/to the process;
- which mediation services are available;
- how and under what circumstances they can claim reimbursement for their costs related to their participation in the criminal proceedings.

***Right to receive proof of complaint***

A victim who reports a crime or fills a complaint with the competent authority is entitled to receive a complain or report receipt.

***Right to translation***

Any documents and acts part of the criminal process are, as a rule, in the language of the country where they take place. It is a right enshrined in the Directive and, subsequently, of any victim in any Member State that they can participate in the criminal proceedings orally and/or in writing in a language they understand. Therefore, the responsible authority for a given criminal process act must request the assistance of an interpreter or translator who understands both the language of the proceedings and the language of the victim. Depending on the role the victim takes in the proceedings, that is, a civil party or assistant, they have the right to receive translations in a language they understand of all the information in the criminal process essential for the exercise of their rights. When the victim has a disability, they are entitled to receive interpretation in a form that enables them to participate effectively in the process, i.e. to request a sign language interpreter or to request a written response to oral questions.

***Right to access victim support services***

The victim has the right to access victim support services, made available free of charge and confidentially, even if the victim has chosen not to make a formal complaint or to report the crime.

***Right to be heard***

During the criminal proceedings, the victim has the right to be heard, to make available information important for the investigation and to provide evidence. Nevertheless, the victim must, at the time of reporting the crime or making a complaint, make available as much information and relevant evidence as possible to the responsible authority. Nevertheless, during the investigation phase, the victim can add additional elements when summoned to make statements to the public prosecutor. Furthermore, if the perpetrator of the crime is charged (defendant) and the case goes to court, the victim can add additional or missing information and answer questions raised by the various parties involved in the case.

It is also possible that the victim, because of their particular vulnerability, will be heard during the investigation phase, and their testimony will be recorded and used in later stages of the criminal process, thus avoiding a repetition of the victim's testimony.

***Rights if the defendant is not accused***
If, at the end of the inquisition phase, the Public Prosecutor's Office finds that there is insufficient evidence to indict and bring the accused to trial, the criminal case is dropped. If several crimes have been committed, the accused may only be indicted for some of the crime(s) and the case will be dropped for the remaining crime(s).

In this circumstance and if the victim disagrees with the decision, they have the right to submit an application to the investigating judge requesting the opening of an investigation. The victim may also apply for a re-examination of evidence or for the investigation to continue, to which they can submit new evidence(s).

***Right to mediation services***
In situations of low and medium severity, such as criminal threat, minor injuries, assaults or others, the law allows the case to be resolved through mediation between the victim and the accused, if the latter has acknowledged committing the crime.

The mediation process should be free, confidential and voluntary, i.e. the victim can choose either to participate or not at any time.

This process' purpose is to provide a communication space, supported and facilitated by an impartial interlocutor, so that the victim can convey the impact and/or the damage(s) caused by the crime and the accused can take responsibility for the act.

The mediator is a professional specifically trained on mediation, and their assignment is to facilitate the communication between the participants.

***Right to information or legal protection***
The system of access to the law and to the courts is designed to ensure that no one has difficulties or is prevented, due to their cultural or social condition, insufficient economic means or knowledge, from exercising and defending their rights.

Thus, the victim is entitled to legal advice on their role in the criminal proceedings. If the victim is an assistant or a civil party, or if the victim wishes to be accompanied by a lawyer and does not have the financial means to do so, they are entitled to legal aid, which may consist of: total or partial waiver of the legal fee payment; appointment and payment of a lawyer's fees; phased payment of the legal fee or the lawyer's fees.

***Right to compensation for participation in the proceedings and reimbursement of expenses***
Any victim who participates in a criminal case is entitled to compensation for their participation time, as well as to reimbursement of the expenses incurred as a result.

***Right to restitution of property***
If any objects or other property owned by the victim are retained by the competent authority(ies) as evidence and are no longer necessary for the criminal proceedings, they must be returned without delay. This return should take place as soon as possible, so that the victim is not deprived of their property longer than strictly necessary for the purposes of the criminal process.

***Right to compensation***
Anyone who suffers damage as a result of a crime has the right to compensation.

The duty to compensate falls on the offender or, in circumstances where the crime leaves the victim in economic difficulties or does not allow the victim to be compensated in time by the offender, an application may be made to the State for an advance payment of their compensation.

***Right to protection***
Victims and their relatives are entitled to protection against acts of retaliation, intimidation or continued criminal activity against them. They have the right to be protected from acts that could endanger their life, physical integrity, emotional and psychological well-being and their dignity when giving evidence.

Where authorities consider that there is a serious threat of acts of revenge or strong evidence that the safety and privacy of the victim may be seriously and intentionally disrupted, an adequate level of protection should be ensured for the victim, as well as their family or other close persons.

The protection and security of victims can be safeguarded by applying one or more coercive measures to the accused as restrictions on the accused's freedom, which can be applied in the course of criminal proceedings, if there is a danger of absconding, a danger of obtaining and retaining evidence of the crime, a danger to public order and/or a danger of continuation of criminal activity.

Where the victim's life or that of another witness, their physical or mental integrity, freedom or property of considerable value is endangered because of their contribution to the investigation and prosecution of the crime, they can require the application of protection meaures.

***Rights of victims with special protection needs***
A victim with special protection needs is someone, because of their personal characteristics, the type or nature of the crime suffered and/or the circumstances in which it occurred, particularly vulnerable to further victimisation, secondary victimisation, intimidation or retaliation, and therefore needs special care, especially protection.

This vulnerability should be assessed on a case-by-case basis, but particular attention should be given to victims who have suffered considerable harm because of the severity and seriousness of the crime, to victims of crime motivated by discrimination based on personal characteristics and to victims whose relationship and dependence on the offender make them particularly vulnerable.

Consequently, victims of terrorism, organised crime, people trafficking, gender-based violence, violence in intimate relationships, sexual violence and hate crimes deserve special attention. Regardless of the type of crime suffered, children, the elderly and people who are ill or have disabilities should be given particular consideration when assessing vulnerability.

***Right to be forgotten***[98]
This right provides its holder with the possibility to request, verbally or in writing, the data controller to delete their personal data. This right can be exercised whenever personal information is considered inadequate, irrelevant or has lost its relevance.

#### 3.5.1.2. The importance of preserving digital evidence

"*The evidence has the function of demonstrating the reality of the facts*" (Article 341 of the Portuguese Civil Code) and "the object of evidence pertains to *all the facts legally relevant to the existence or non-existence of the crime, the punishability or non-punishability of the accused and the determination of the applicable custodial sentence or detention order*" (Article 124(1) of the Portuguese Code of Criminal Procedure). If there is a civil request, the facts relevant to determining civil liability (Article 124(1) and (2) of the Portuguese Code of Criminal Procedure) *constitute the object of evidence*. Regarding the principle of legality of evidence, in the Portuguese legal system, Article 125 of the Code of Criminal Procedure states that "*evidence which is not prohibited by law shall be admissible*".

Because these are crimes that occur in the digital world, their investigation faces several obstacles (Martellozzo & Jane, 2017). Studies and researchers focussing on the analysis of **cybercrime** and of the difficulties in the **reporting/complaint**[99] **and investigation of cybercrime** have indicated, among others, the following obstacles:

- the 'place' where the criminal conduct took place;
- the identification of the perpetrator (especially due to the anonymity provided by the cyberspace ecosystem and the impermanence and volatility of evidence on their behaviours, which can be easily blocked, modified, rendered useless or erased);
- the establishment of causality in cases often involving multiple and diffuse perpetrators and victims.

In other words, these difficulties in the investigation are shown by the fact that this type of crime is transnational, anonymous and variable (constantly evolving and with new forms of action emerging constantly) (Santos, 2016; Holt & Bossler, 2015).

[98] This right, unlike the previous ones, is not part of Directive 2012/29/EU. It is included in Article 17 of the General Data Protection Regulation. For additional information, see Part I, Chapter 2, section 2.2 of this Handbook.

[99] See Part I, section 1.4 of this Handbook for this purpose, which deals with the difference in the number between crimes reported and those actually committed associated with cybercrime and the grounds for not reporting cybercrime.

HIGHLIGHT | PRACTICES IN FOCUS:

The *SIRIUS* Project, led by *Europol's European Counter-Terrorism Centre and the European Cybercrime Centre*, in partnership with Eurojust and the European Judicial Network, aims to help authorities deal with the complexity and volume of information in a rapidly changing online environment.

This project aims at sharing knowledge through events and a restricted platform where Member States (and third countries with an operational agreement with EUROPOL) can find up-to-date information and access digital evidence for criminal investigation.

Additional information is available at: www.europol.europa.eu/sirius

Regarding evidence, the use of ICT in criminal activities has popularised digital evidence (Balkin et al., 2007).

Indeed, one of the most significant differences between cybercrime and *traditional* crime concerns the nature of evidence. There are differences in the form it takes, the way it is stored, where it is located and how it can be found. In addition, digital evidence is intangible, generally volatile, and its amount can also be massive, which poses substantial logistical challenges (Grabosky, 2007).

Since digital evidence is temporary and highly volatile, there are additional challenges to ensure its validity and safeguard other relevant characteristics, that is, it is essential to ensure that the evidence is admissible, authentic, and accurate and complete (Marques, 2013). As an example, a simple non-conformity in the storage of evidence and the consequent breaking of the chain of evidence can nullify it and make it legally inadmissible (*idem*).

Digital evidence, like other types of evidence, must be manipulated so as to preserve their probative value, which relates not only to its physical integrity but also to the data it contains. Depending on the type of device, special measures of collection, packaging, transport and storage must be implemented (*idem*).

#### 3.5.1.3. The role of interinstitutional cooperation

Considering the nature of intervention with victims of cybercrime and the response to their identified support needs, which are often associated with the criminal process, it is important to consider **inter-institutional coordination between the victim support organisations and services and the police and judicial authorities**.

Ideally, these inter-institutional collaborative processes could be conducted through formal partnerships via **protocols and cooperation agreements**, which enable the joint definition of procedures and collaboration, in order to streamline communication and information-sharing mechanisms that

contribute to better support, treatment and intervention to victims of crime in general and to victims of cybercrime in particular.

HIGHLIGHT | PRACTICES IN FOCUS:

The Portuguese Association for Victim Support (APAV) and the Portuguese Judiciary Police, an authority that in Portugal has reserved competence in the investigation of cybercrime, signed a cooperation protocol in 2019 for their collaboration within the scope of the Safe Internet Line (in Portuguese: *Linha Internet Segura*).

The Safe Internet Line, operated by APAV under the Safe Internet Centre consortium, is a telephone and online support service with two components: advice and information on issues related to the use of the Internet and ICT, as well as support and information in cybercrime situations (Helpline); reporting illegal content on the Internet (Hotline).

This cooperation protocol also covers the establishment of a referral system to APAV for cybercrime victims served by the Judiciary Police, and it enables information related to cybercrime complaints received by the Secure Internet Line to be transmitted efficiently to the Judiciary Police.

In general, and as the example above confirms, these protocols and agreements promote setting up and implementing **mechanisms for referral of victims of crime**.

Regarding this, the previously mentioned Directive 2012/29/EU advises facilitating the referral of victims of crime by the competent authorities to victim support services in order to ensure the victim's **right to access support services before, during and for an adequate period after the conclusion of the criminal process**.

Following from this, we see the referral **process** as a **mechanism of interinstitutional collaboration** in which one organisation transmits information about the occurrence of crimes and their victims to another organisation, with the victim's consent and for providing them with support. Referral is based on proactive processes which is integral to the support procedures for victims of crime of a given service or support organisation. Referral always implies respect for the victim's will and consent and promotes the victim's access to more specialised or specific support, which will best meet previously identified needs.

HIGHLIGHT | INFORMATION IN FOCUS:

The way information is collected and transmitted, aiming at victims referral, must also be established and agreed between the organisations involved in a particular referral mechanism.

Regardless of the method(s) for collecting and transmitting information, it is essential that the information transmitted allows the identification of the victim and understanding the situation of victimisation, minimising the risk of the victim having to report again the episode(s) that led to the contact with the service or support organisation.

The following background information should therefore be included in any referral process:

- Victim's name;
- Victim's contact and preferred time for contact;
- Brief description of the crime/situation of victimisation (type of crime; relationship to offender, where applicable; consequences and impact of victimisation);
- Observations and support provided by the organisation (e.g. psychological support, legal information and other observations relevant to the organisation to which the victim was referred).

HIGHLIGHT | PRACTICES IN FOCUS:

*Project VICToRIIA - Best Practices in Victims Support: Referrals, Information, Individual Assessment*, promoted by the Centre for Crime Prevention in Lithuania (NPLC), with the financial support of the Justice Programme of the European Union, aimed the development of referral mechanisms between victim support organisations and law enforcement. Amongst its activities a *Manual of effective and secure referrals of victims* was developed.

Among several reccomendations for effective and secure referral procedures for victims, it is highlighted the importance of preserving vicitims' safety, but also guaranteeing that vicitms' personal data is protected as per the EU's General Data Protection Regulation (GDPR) and any relevant national laws.

Additional information at: http://nplc.lt/victoriia/.

### 3.5.2. Psychological support: objectives and fundamental aspects

Psychological support aims at providing a therapeutic experience for the victim and/or the family and to minimise the negative effects of exposure to an adverse and potentially traumatic experience. It thus responds to the victim's and/or their family need to restore their psychological and emotional functioning and well-being affected by the victimization experience (APAV, 2013).

Psychological support should be delivered exclusively by professionals with a psychology degree and whose qualifications and experience have been duly recognised, where applicable, by the country's respective regulatory entity, which regulates access to the profession and the professional activity.

There are several models and schools used in the psychological intervention with victims of crime, including psycho-dynamic therapies, cognitive-behavioural interventions and narrative and constructivist therapies. Regardless of the support professional and their organisation's preferred theoretical approach, knowledge about the different forms of cybercrime and their dynamics, as well as the risk factors associated with cybercrime and their impact on the psychological, emotional and social functioning of the victim is fundamental[100].

The main objectives of psychological support are:

- Relief and improvement of symptoms;
- Reducing discomfort and dysfunctional behaviour;
- Strengthening adaptive defence mechanisms;
- Improving adapting to the environment;
- Improving ability to judge reality;
- Increasing self-esteem;
- Maximising autonomy;
- Restoring psychological balance.

In the following sections, we present guidelines and some of the generic key aspects to consider when delivering psychological support responses to cybercrime victims. The content covered does not represent a referential or psychological intervention programme with victims of cybercrime; rather, it proposes assumptions and principles that should be taken into account in any intervention process in this area, regardless of the theoretical approach used and the organisation providing support.

#### 3.5.2.1. Requirements and operating principles of psychological support

Some of the **requirements** that should be considered for the success of psychological intervention with the victim are (APAV, 2013; Alexy et al., 2005):

- The professional should establish a therapeutic alliance and a supporting relationship with the victim, without stigmatisation and prejudice;
- The professional should adequately assess the impact of the cyber-victimisation experience, particularly the indicators of psychological, emotional and behavioural maladjustment, including avoidance and re-experience (symptoms associated with traumatic post-stress), social functioning and professional behaviour, and the risk of suicide;

[100] See, for this purpose, Chapters 1, 3 and 4 of Part I of this Handbook, in which the typologies and different types of cybercrime, socio-demographic risk factors and behavioural risk factors associated with the experience of cybercrime and the consequences of cybercrime are explored.

- The professional should also assess possible comorbidities[101] with other mental disorders or conditions, referring the victim to other professionals and/or more specialized services, if necessary;
- The questions must be timely and sensitive, making the victim's verbal account easier;
- The professional should validate the victim's feelings, thoughts and history of victimisation;
- The professional should help the victim to deal with adverse emotions and feelings associated with the cyber-victimisation experience, such as fear, anger, guilt and shame;
- The professional should provide information about the possible reactions to the cyber-victimisation experience, being able to frame the victim's thoughts, feelings and behaviours as normal reactions and consequences to unexpected life events, promoting positive expectations regarding the recovery process;
- The professional should help the victim to find strategies to diminish cognitive and behavioural avoidance and to deal effectively with the possibility of reviving the event and the occurrence of intrusive thoughts, such as feelings of inefficiency, incompetence and hopelessness, as well as anger, guilt and shame, promoting increased self-esteem and the establishment of trusting relationships.

The following **operating principles** should also be taken into account (APAV, 2011; APAV, 2013):

***Therapeutic contract***

At the beginning of the support process, a set of rules and procedures should be agreed with the victim - the *therapeutic contract*, defining the time, frequency and duration of sessions, the rules of attendance and punctuality, as well as presenting the objectives and planning for the intervention. This contract also aims to ensure the committment and responsibility of the victim towards the psychological support process and the resulting successes, contributing to the victim's engagement and compliance with the intervention objectives.

***Neutrality and anonymity***

The professional should communicate and interact with the victim without personal opinions, self-revelations, manipulations and other inappropriate responses of psychological support. They should promote the victim's free emotional and affective expression, without embarrassment.

Neutrality does not mean lack of empathy, and this competence is very important to build a relationship of trust between victim and support professional, as mentioned previously[102].

***Privacy and confidentiality***

The victim must be assured that the information shared in the context of psychological support will always be kept within the scope of the intervention. The transmission of information to third parties (persons or organisations) about the psychological support will only take place following the victim's prior consent provided for this specific purpose.

[101] Comorbidity means that two or more disorders co-occur in the same person.

[102] For additional information on communication and empathy in contacts with victims of crime and cybercrime, please refer to Chapter 2 of this part of the Handbook.

### 3.5.2.2. Phases of the psychological support process

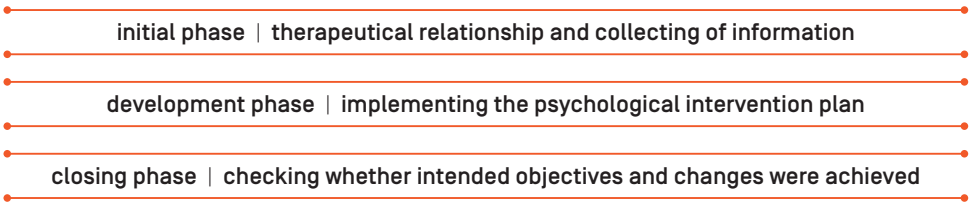


Figure II- 5: Phases of the psychological support process

***Initial phase of the psychological support process***

This phase is aimed at **establishing a relationship of trust** between the victim and the support professional responsible for the psychological intervention. The professional's personal and technical skills, as well as their empathic communication competences (see sections 2.1 and 2.2 of Chapter 2 of Part I of this Handbook) are fundamental here. It is at this point in the support process that the therapeutic contract is established.

In the initial phase of this intervention process, **information gathering** and analysis should take place and inform a plan and strategies for psychological intervention.

In this regard, the collection of information from the victim of cybecrime[103] by (possibly) other support professionals, in previous contacts with the organisation, can be useful, since it provides a global understanding of the victim's life history, internal and external resources, as well as the experience of cybercrime and its impacts.

Additionally, the professional can use **scripts and interviews to collect information and psychological assessment tools** in order to record and systematise the relevant information for setting up the intervention (particularly to respond to the victim's requests and their emotional and psychological needs) and to analyse specific areas of psychological and emotional (dys)functioning. The collection of information from victims should be complemented by observating their behaviour and their **non-verbal communication and language**, which are important indicators on the victim's emotional state and their well-being and functioning.

Collecting information for defining the psychological intervention can be, in itself, a therapeutic process – while it allows mapping the (internal and external) resources affected by the cyber-victimisation experience, it also contributes to the victim's free emotional expression and to the development of a narrative around the cyber-victimisation experience.

[103] Additional information on the importance of collecting information is available in Part II, Chapter 2, section 2.3 of this Handbook.

***Development phase of the psychological support process***

This phase is marked by the **implementation of the psychological intervention plan and strategies** previously defined, and can take place over several occasions or sessions. It also continues the collection and analysis of information, seen as a circular and cross-cutting intervention process.

Regardless of the intervention strategies and the theoretical orientation/school used, when implementing the psychological intervention plan, the supporting professional should seek to:

- **Facilitate emotional expression and communication**: the professional should motivate the victim to share their feelings, emotions and thoughts, assuring them and showing that this can be done without them being judged;
- **Promote the victim's understanding of their problems and responses**: the professional should explain to the victim the type of crime they were subject to and present similar cyber victimisation situations, making it easier for the victim to identify these with their history of victimisation and, subsequently, with the associated needs and problems and possible solutions;
- **Showing interest and empathy**: on this subject, see Part II, Chapter 2, sections 2.1 and 2.2 of this Handbook;
- **Strengthening self-esteem**: Strengthening the victim's self-esteem contributes to the promotion of the intended behaviour changes;
- **Facilitating problem solving**: the professional should help the victim to face difficulties, to make decisions and to solve problems by guiding them to solutions.

***Termination phase of the psychological support process***

Since it is difficult to determine the right moment to end the psychological support process, the professional should review with the victim the intervention plan objectives developed at the start to:

- Find out which meaning the victim assigns to their experience of cyber-victimisation and to what extent they consider that the objectives have been fully or partially met;
- Anticipate prevention and protection strategies;
- Confirm which skills the victim has acquired to maintain improvements and changes achieved through the intervention process.

After ending the process, it is important that the professional ensures a **follow-up** of the case to collect information on whether the results obtained after the psychological support has ended are still maintained.

Regardless of the moment or phase of the psychological support process, the following table presents some communication techniques that can help to achieve the interventions' objectives (APAV, 2013).

.

**Table II-7: Useful communication techniques and strategies for the psychological support process**

| |
|---|
| **Catharsis** - facilitating the expression of feelings and emotions |
| **Questioning** - asking closed questions (e.g. "What's your name?") or open questions (e.g. "What do you think about it?") to obtain information |
| **Restructuring** - reorganising the information shared by the victim in a different way, allowing a change of perspective on the subject |
| **Focus** - select, from the information shared by the victim, the most relevant for a given intervention objective |
| **Interpretation** - adding meaning to something that was expressed by the victim |
| **Clarification** - to clarify what was said by the victim, for a better understanding of their symptoms, feelings and behaviours |
| **Confrontation** - comparing discrepant content on the same topic to clarify doubts, incongruities and/or challenge victim's verbalisations or behaviours |
| **Suggestion** - Inducing an idea or feeling to suggest alternative scenarios |
| **Echoing** - repeating a word or question about some information shared by the victim, as a way to keep the victim's attention to the intervention process and strengthen empathic communication and the relationship between the professional and the victim |
| **Silence** - serves mainly to ensure time for reflection |
| **Securing self-esteem** - reassuring and reinforcing the victim's self-esteem by expressing agreement with an idea, thought, attitude or decision |
| **Counselling** - presenting attitudes or decisions in order to reinforce healthy aspects of the victim's behaviour, reduce symptoms or avoid crises |
| **Education** - Clarifying relevant issues or situations |

### 3.5.3. Social support: objectives and fundamental aspects

According to the International Federation of Social Workers (2005 cit. in APAV, 2013), social work includes promoting social change, problem solving in the context of interpersonal relations and people's ability to improve their well-being. Social work thus seeks to bring about **positive changes in the psychological and social functioning of people, groups and communities**, reducing vulnerabilities and providing opportunities for a more satisfactory social life.

Social work purposes are:

- Promoting the inclusion of vulnerable or at-risk social groups;
- Promoting well-being and solving problems by intervening with people, groups and communities;
- Initiating protection procedures for people who, due to their condition or situation, are not able to do that autonomously.

Social work therefore extends to very diverse areas such as education, information and guidance, psychosocial support and management of services or equipment (APAV, 2013).

Social Support is under the responsibility of SocialWworkers, but also Social Policy professionals and other duly qualified professionals in the Social Work area (*idem*).

As with other specialised forms of support, social support for victims of cybercrime requires that the professional, in addition to their academic training, knows and masters the theoretical and conceptual framework of the needs of cybercrime victims. Moreover, theyr should have adequate knowledge and mastery of the characteristics and dynamics associated with the different types of cybercrime and their impact on victims[104].

#### 3.5.3.1. From social diagnosis to individualised intervention

**Social diagnosis** is a process of elaboration/systemization of information about a context, understanding its problems and needs, as well as the causes and their evolution. Through social diagnosis, it is possible to set priorities and intervention strategies, **involving the available resources and social actors** (Ander-Egg & Idánez, 1999 cit *in APAV*, 2018).

Social diagnosis should be one of the first phases of social support. It represents a continuous process, aiming at the knowledge of the reality experienced by a certain person, group or community, as well as its constant evolutions/modifications, therefore requiring a constant collection and analysis of information.

**Social diagnosis is a basic step for an individualised intervention** with the victim of crime and cybercrime. Only after diagnosing the victim's relational, social and institutional situation, should the professional design the intervention, involving the victim and their primary support network, as well as the formal support structures (García & Romero, 2012 cit *in APAV*, 2018). This approach to individualised intervention is called Case Method.

The Case Method can be summarized in four basic steps (*idem*):

- Study and diagnosis of the problem;
- Program/ Intervention design;
- Delivery/implementation of the intervention;
- Evaluation.

In order to achieve these four stages, which will produce an individualised intervention focussed on the victim's relational, social and institutional needs, the professional should:

[104] See Chapters 1, 3 and 4 of Part I of this Handbook, which explore, respectively, the typologies and different types of cybercrime, the risk factors associated with the experience of cybercrime, the consequences of cybercrime and the needs of cybercrime victims.

**Table II-8: Indivualised intervention and victims needs**

## Identify the crime

The identification of the victim and the crime can be based on the information gathered from other contacts between the victim and the organisation[105], and includes the experience/history of cyber-victimisation, information on the victim, their characterization and the pre-victimisation history.

## Assess the victim's needs

The assessment of the victim's individual and social needs should be centred on their interests, according to their context of life and considering their case's specific problems.

The professional must:

- Allow the victim to express what they want and what they need;
- Clarify and reformulate the needs expressed to ensure a correct understanding;
- Continuously provide information on existing rights, resources and support services that enable victims to identify their own needs;
- Continuously evaluate the different needs and their levels of urgency in order to respond to the most pressing.

Urgent needs include: safety, basic needs, medical and/or psychological care, shelter and legal support.

Medium and/or long-term needs may include: financial support, supporting their education, (re-)integration support, skills training and occupational integration.

As a rule, social support needs can be grouped under the following dimensions:

| | |
|---|---|
| **SHELTER** | Situations of relationally-motivated cybercrime enabled via the Internet and ICT, such as cyberstalking and the non-consensual dissemination of images and videos in situations of violence in intimate relationships, can require shelter, either urgent/emergency or planned support.<br><br>The professional should prepare a situation diagnosis (identify the primary support network - friends, relatives and other trusted people - or the need to activate secondary support networks) and assess the situation's degree of risk. Support can take place in the primary support network, if it meets the necessary safety conditions. It can also be institutional, which requires being aware of the shelter available at local/regional/national levels, and referral to social emergency lines, shelter structures/responses, non-governmental organisations, social security services, among other available responses/resources. |
| **FOOD** | The cybercrime victim, for example, in online scams, may find themselves in situations of economic insufficiency and unable to meet basic needs such as food or medication for pre-existing health problems.<br><br>The professional should map the various institutions in that area of intervention, their objectives, procedures and operating rules, in order to refer the victim adequately, accompanying them when contacting these other organisations.<br><br>For this purpose, the professional should know the organisations in their own country that can be contacted for addressing these needs, and eventually make referrals to non-governmental organisations, social security services, religious institutions, among other available answers/resources. |
| **HEALTH** | The experience of cyber-victimisation can lead to physical or mental health needs.<br><br>The professional should be able to identify the most appropriate organisations and responses in |

[105] See Part II, Chapter 2, point 2.3 of this Handbook for that purpose.

| | |
|---|---|
| | their own country, and eventullay make referrals to health /emergency lines, state-funded health services, non-governmental organisations, religious bodies or other health responses (including private health services). |
| OCCUPATIONAL SITUATION | In view of the potential effects of cybercrime on the victim's professional situation, it may be necessary to find a new way of ensuring their livelihood. Professional (re-)integration becomes essential in order to allow a higher level of autonomy. The professional should assess the victim's academic qualifications, their professional experience, their preferences regarding the the labour market sectors and possible training needs. The professional should refer the victim to competent bodies, such as employment and vocational training centres, which can help and promote professional reintegration. They should also facilitate the victim contacting human resource departments in working areas that fit the victim's profile, skills and work interests. |
| EDUCATIONAL/ TRAINING SITUATION | Cybercrime can affect the child or young person victim's educational situation in situations such as cyberbullying, online child sexual abuse and exploitation, or children and young people under the care of the direct victim of cybercrime (if this applies to the specific case). It is important that the professional liaises with the current training or education institutions in order to implement actions addressing the victims' direct and indirect training needs, such as the transfer to another school or training programme, which should be done discretely to guarantee the safety of direct and indirect victims. |

## Referring and working collaboratively

These basic needs (and the responses to them) are important areas of intervention in terms of social support.

Given the identified needs and the scope of action of the professional's organisation, it may be necessary, as mentioned above, to refer the victim and to collaborate with other organisations/services in the community. The professional (and their organisation) should have, for each area of intervention, contacts of existing secondary support networks at regional and national level, which may be activated for supporting the needs of crime victims.

In order to respond to the needs of the victim and to maximise the quality of the support provided, it may therefore be necessary to liaise with other sectors/areas[106], in particular:

- Social Security and Social Protection (such as social security services and private charities/non-governmental organisations);
- Work and unemployment (including employment and vocational training centres);
- Human resources departments of companies and other local organisations or committees;
- Health (such as hospitals, health centres/units and mental health institutions);
- Education and/or Training institutions;
- Local authorities (e.g. town councils and parish councils);
- Justice (such as police forces, courts and forensic offices);
- Communication and ICT (including telecommunications operators, Internet Service Providers, social network platform providers and other information sharing platforms);
- Economics and finance (such as banks, credit institutions and payment and electronic transfer companies or platforms).

Liaising with these services can take place as a referral[107].

[106] Regarding cooperation at a multi sectorial level, please consult the already mentioned WePROTECT Global Alliance, at https://www.weprotect.org/, as they proposed a comprehensive model to act against online child sexual abuse and exploitation.

[107] For more information on referencing and referral, please refer to Part II, Chapter 3, point 3.5.1.3 of this Handbook, where the importance of interinstitutional collaboration is addressed.

#### 3.5.3.2. Key aspects for the success of collaborative work

Interinstitutional cooperation is important in supporting victims of cybercrime, regardless of the support under consideration, and is particularly relevant in addressing identified social and institutional needs following a victimisation experience (or cyber-victimisation, in this case).

HIGHLIGHT | INFORMATION IN FOCUS:

At the *Policy Paper: challenges in the field of cybercrime and recommendations to overcome them*, developed under Project ROAR: empowering victims of cybercrime[108], a set of recommendations to be taken into account when designing cybersecurity holistic strategies are proposed. Multi-sector cooperation for a victim-centred approach, involving, policy makers, law enforcement agencies and judicial authorities, victim support organisations, industry and media and communication agencies, is emphasised as a means to properly respond to the victims' needs and the challenges of tackling cybercrime.

Working collaboratively with professionals from other institutions and services is fundamental to the quality of the treatment provided to any victim of crime.

The professional should work in constant collaboration with professionals from other institutions and services to ensure correct support and adequate response to the victim's interests and needs. The professionals should:

- **Facilitate**, by promoting effective communication and a satisfactory relationship between the professionals from different services and institutions;
- **Stimulate**, by engaging those professionals in solving/minimizing the consequences of crime or cybercrime and to respond adequately to the victim's needs.

Integrated action can prevent some of the constraints that affecting interinstitutional collaboration:

**Formality.** The negative effects of an excessive formality on the daily contact between the institutions (e.g. excessive bureaucratic procedures) should be reduced, as this can be detrimental to the support process, particularly the speed and efficiency in solving the problem.

**Time.** The time available to meet a certain requirement of the process (e.g. sending a referral report quickly) should be managed effectively without delaying or undermining the work of other services and institutions.

**Lack of practical sense.** A practical view of the support process requirements should be promoted when contacting other institutions.

[108] Additional information about the Project's activities and outputs may be found at https://apav.pt/publiproj/index.php/96-projeto-roar

**Lack of cordiality.** The professional should be polite to all professionals in the support process they are in contact with (e.g. on the phone, in person, by email, etc.).

**Communication errors.** Ambiguous communications that lead to a misunderstanding of messages or requests should be avoided, as these can affect the relationship and cause considerable damage, influencing the quality of support provided to the victim.

**Insufficient information sharing.** Insufficient information shared with professionals from other institutions or services should be avoided, as this may limit or delay their work in the supporting process (e.g. sending a careless, omissive or unclear report that does not have the necessary information to progress with the process).

**Reductive and isolated intervention.** A global vision should be adopted in the support and referral of victims, promoting networking through the active participation of other professionals outside the service or institution, optimizing the available resources.

**Negative competition.** A culture of competition with other services and institutions should not be promoted; rather one should promote a culture focussed on maximising resources and skills of other services and institutions in order to promote an appropriate and quality intervention.

**Lack of personal contact.** Finally, one should contact professionals from other institutions and services personally, promoting close working relationships between all, in order to ensure more easily the necessary steps in the intervention with victims.

# 4. THE IMPORTANCE OF PREVENTION IN COMBATING CYBERCRIME

In general, **crime prevention** is defined as all private and/or public initiatives and efforts that aim to prevent crime by reducing its risk of occurrence by changing the risk factors and/or, when this is not possible, by mitigating its effects on people and society (Copibianco, 2010, Welsh & Farrington, 2012 *cit in Maia* et al., 2016).

The first attempts in crime prevention come from Public Health approaches, and the concept of *prevention* (of disease or injury) was later appropriated by other areas of social and community life (Bloom, 1996, Doll, Saul, & Elder, 2007 *cit in Saavedra* & Machado, 2010) and even transposed to issues related to security, violence and crime.

## 4.1. Approaches to cybercrime prevention: key aspects

Following the prevention concept mentioned above and a public health approach (APAV, 2011), prevention can be categorized according to its ***timing*** (or by the evolution of the condition) in the following dimensions:

- **Primary prevention:** intervention prior to the problem, to prevent the onset of illness or injury.
- **Secondary prevention:** intervention aimed at treating the problem, which has started, at the earliest possible stage.

  Transposing to issues of violence and crime, secondary prevention concerns approaches focusing on immediate reactions to crime and violence (e.g. medical care; emergency services).
- **Tertiary prevention:** intervention focused on preventing relapse, preventing the frequency and severity of damage.

  Tertiary prevention, when applied to issues of violence and crime, includes approaches focused on long-term care after violence or crime, such as rehabilitation, reintegration and reduction of trauma/consequences associated with crime/violence.

Although traditionally secondary and tertiary crime and violence prevention approaches are used in the intervention with victims, they are also considered relevant to the intervention with perpetrators of crime or violence, particularly in the context of the judicial sector responses.

Prevention can also be defined according to the ***target group of interest*** or ***population*** for which it is intended (APAV, 2011), and categorized as:

- **Universal prevention:** approaches that target groups or the general population, regardless of the level of risk.

Examples of universal prevention approaches include violence prevention programmes for children and young people at a certain school level as well as awareness-raising campaigns targeted at the population.

- **Selective prevention:** approaches aimed at groups/persons considered to be at higher risk of involvement in violence or crime compared to the general population.

  Examples of this intervention approach include programmes to promote parenting skills for single parents.

- **Indicated prevention:** intervention approaches for high-risk people/groups who have already demonstrated some involvement in situations of violence or crime, either as victims and/or perpetrators.

  For example, indicated prevention approaches may include intervention programmes for persons accused of domestic violence and the support responses for victims of crime and violence provided by victim support organisations.

There are also other types of classification of prevention strategies, namely according to the ***prevention focus*** (e.g. UN, 2011 *cit in* Maia et al., 2016; Tonry & Farrington, 1995 cit *in Maia* et al., 2016):

- **Crime prevention through social development**, focusing on increasing protective factors and reducing crime risk factors, which may include, for example, social skills development programmes for children at risk.

- **Community or local crime prevention**, focusing on intervention in geographical areas with a higher risk of crime and promoting a sense of security.

- **Situational crime prevention**, which refers to the reduction of opportunities to commit crime, the increase of risks/costs associated with committing it, and the reduction of benefits.

- **Criminal prevention via criminal justice**, which could include reintegration and repeated offenders' prevention programmes.

Apart from community or local crime prevention strategies, the other approaches to crime prevention mentioned above can be translated into **cybercrime prevention**. It is important to note that cybercrime prevention efforts often focus on technology and the protection of computers and devices, while crime prevention models focus primarily on the human factor.

Regardless of the approaches to prevention and typologies summarised above, the Public Health approach[109] is useful to help organisations understand and implement strategies to prevent crime

[109] Detailed information on the Public Health Approach to crime and violence prevention as well as resources to support the planning, implementation and evaluation of prevention measures are available at https://vetoviolence.cdc.gov/apps/main/home

and violence. Despite the complexity of prevention, we can organise the planning, preparation and implementation of prevention strategies into four macro-stages:

| | |
|---|---|
| **1 problem definition** | • requires **understanding the phenomenon** and its dynamics and identifying its **magnitude and expression** (e.g. statistics on the number of reports/complaints on a specific crime) in a specific group, community, region or country |
| **2 identification of risk factors and protective factors** | • **risk factors**: characteristics or conditions that can increase the likelihood of a certain problem<br>• **protective factors** : characteristics or conditions that can decrease the likelihood of a certain problem<br>• prevention strategies should reduce risk factors and increase protective factors |
| **3 develop, test and evaluate prevention strategies** | • prevention strategies should be evidence-based, take the diagnoses that were conducted into account as well as the problem to be addressed and associated risk and protective factors<br>• **monitoring** the prevention strategies and **evaluate their effectiveness** are key steps |
| **4 publicise and generalise** | • after analysing the results of the prevention strategies implemented, it is fundamental to **publicise** them to allow their use by other organisations |

Figure II-6: Stages for the planning and implementation of prevention strategies

In addition, and regarding cybercrime prevention, Askerniya (2012)'s proposed model for **organising cybercrime prevention strategies** has four key dimensions, all of them including awareness and education as critical elements in the reduction of cybercrime (Jahankhani, 2013 *cit in* Al-Ali et al., 2018):

1. **Individual users' level of technical knowledge** is the first dimension of cybercrime prevention interventions. In order to reduce individual risk and improve personal protection, interventions should focus on educating, raising awareness and training users on the specific skills needed for a safe participation in different online activities (such as downloading music, games and films, online shopping and/or using social networks).

2. The second dimension concerns the reduction of exposure to cybercrime risk through **prevention strategies adapted to different individual development stages of the user**. This dimension assumes that the risk of cybercrime is affected by the risk and protective factors associated with individual development, so the user's age/age group is essential for defining and deciding which cybercrime preventive intervention strategies should be delivered.

3. The third dimension concerns the **users' risk levels in their exposure to cybercrime** and the

need for preventive interventions depending on the users' knowledge, training and awareness. Thus:

- **Low risk of cybercrime exposure** is associated with users having considerable knowledge about ICT and the Internet, as well as adjusted levels of awareness about the risks of online exposure.

- **Average risk of cybercrime exposure** is associated with users with insufficient knowledge and awareness of online exposure risks and with a higher risk of cyber-victimisation (compared to the previous category). This dimension includes people who, despite their knowledge about the security of computers and devices, are not sufficiently aware to change their online behaviour and/or their Internet and ICT usage habits.

- **High risk of cybercrime exposure** is associated with users with high rates of intensive Internet and ICT usage, but low awareness of risk exposure.

4. The fourth and final dimension of this model concerns the **promotion of individual skills and behaviours and the development of interventions** based on training, education and risk awareness regarding online exposure risks and and specific behaviours[110].

In the next section we present some cybercrime prevention practices.

## 4.2. Information, awareness and education as prevention strategies

Following the key dimensions of cybercrime prevention strategies presented above, it becomes clear how much impact information, awareness and education of Internet and ICT users have on their behaviour and skills, and consequently, on increasing/reducing the risk of exposure to cybercrime.

Internet and ICT users' perceptions of their own **abilities and knowledge** to protect themselves from cyber-victimisation affect their behaviour and online activities. The same applies to responsibility for personal online security (Boehmer et al., 2015; LaRose & Rifon, 2007). That is to say, people who consider cybersecurity to be a personal responsibility and/or who understand that they have the knowledge and skills to protect themselves from cyber-victimisation are (probably) adopting more cybersecurity measures and more personal protective behaviours when using the Internet and ICT.

This interpretation highlights the need for **information and awareness campaigns** and **educational programs** (Martin & Rice, 2011; Burns & Roberts, 2013):

- Information and awareness campaigns should promote the safe and competent use of the Internet and ICT;

[110] For additional information regarding vulnerability as a risk factor for cyber-victimisation, please refer to Part I, Chapter 3, Section 3.2 of this Handbook.

- Educational programs should provide knowledge and opportunities for the training and acquisition of skills needed to adopt online safety behaviors.

In any case, these information, awareness and education strategies should (Bandura, 1997 *cit in* Lee et al., 2008; Boehmer et al., 2015; Saridakis et al., 2016):

- Explicitly inform about the risks to which users may be exposed when using the Internet and ICT;
- Identify and make users aware of personal risk behaviours that may increase vulnerability to cyber-victimisation;
- Raise users' awareness of existing protection and cybersecurity measures, including through objective information on the effectiveness of available protection;
- Teach ways to implement the available protective and cybersecurity measures, e.g. through contextual help and step-by-step instructions;
- Emphasise the positive results associated with adopting safe online behaviour.

While it is true that information, promoting awareness and education strategies can be implemented in any age group, practices and initiatives in this field have been mainly focussed on children and young people.

Below we present a summary of some universal prevention practices for cybercrime, covering initiatives, programmes and projects for children of different age groups, which are based on information, the promotion of knowledge and the strengthening of skills for the safe use of the Internet and ICT.

**Table II-9: Cybercrime prevention programs/projects - COMMUNICATE SAFELY**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target-group** | Children aged 6 to 18, extended to parents and to the elderly |
| **Themes/Problems** | Safe use of the Internet |
| **Objectives** | • Promote ICT competencies<br>• Coporate volunteering Initiative from Altice Foundation aimed at raising awareness of the educational community to the correect use of the ICT, namley the Internet and the mobile phones |
| **Context of Implemetation** | The programme includes awareness raising sessions in classrooms with contents structured by school year and emcompassess all School levels and a theathre play. It is complemented by several online sesources. |
| **Descrição** | Partnership:<br><br>• PSP - Polícia de Segurança Pública<br>• Consórcio CIS - Centro Internet Segura, Portugal<br>• ANPRI – Associação Nacional de professores de Informática<br>• RBE – Rede de Bibliotecas Escolares<br><br>Themes:<br><br>• Parental control<br>• Privacy<br>• Password<br>• Digital ID<br>• Sharing of personal data and images<br>• Cyberbullying<br>• Healthy use<br>• Safety of devices (Mobile Phones and Computers)<br>• Dowload of apps and games<br>• Fraud/ Virus<br>• Online Purchases<br>• Malware<br>• Ransomware<br>• Public WiFi |
| **Country of implementation** | Portugal |
| **Additional information** | https://fundacao.telecom.pt/Site/Pagina.aspx?PageId=1975 |

**Table II-10: Cybercrime prevention programs/projects - THINKUKNOW - "JESSIE & FRIENDS"**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | Children aged 4 to 7 years |
| **Themes/Problems** | Internet Security |
| **Objectives** | • Promote knowledge, skills and confidence for a safe and secure use of the Internet and ICT;<br>• Provide opportunities for learning key principles/values for a safe use of the Internet and ICT: respect for others; consent; healthy and unhealthy behaviour on the Internet; seeking help from trusted adults. |
| **Implementation context** | Can be implemented as a group (in a classroom context, for example) and individually (family context) |
| **Description** | • "Jessie & Friends" is an animated series, with three episodes for children from 4 to 7 years old: (i) episode 1 - 4-5 years; (ii) episode 2 - 5-6 years and (iii) episode 3 - 6-7 years.<br>• "Jessie & Friends" follows the adventures of Jessie, Tia and Mo when they use the Internet and ICT. The characters learn that while the Internet is a place for fun, it is also a place of risk.<br>• The series is accompanied by a Guide for teachers, parents and/or carers, with session guidelines.<br>• It is also complemented by a book with the stories, to reinforce learning at home/family and/or school |
| **Country of implementation** | United Kingdom |
| **Additional information** | https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/ |

**Table II-11: Cybercrime prevention programs/projects - THINKUKNOW - "THINKUKNOW TOOLKIT"**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | Young people 11 years and older |
| **Themes/Problems** | Internet Security |
| **Objectives** | • Develop healthy approaches to issues such as relationships, sex and the Internet;<br>• Identify negative behaviours associated with these topics;<br>• Know where to find advice and guidance on these topics;<br>• Know where to look for help, when faced with online risk situations. |
| **Implementation context** | School context |
| **Description** | Activities carried out:<br>• *Speed finding* - role-playing, which explores the nature of online 'friendship', identifies risks and highlights safe ways to socialize online;<br>• *Digital Tatto* - discussion in pairs and in the group, introducing young people to the concept of "digital tattoo" (or 'digital footprint') and ways to manage it;<br>• *Code Breaker* - activity where young people try to guess the passwords defined by fictional characters;<br>• *Thinkuknow Better?* - young people develop advice to support their peers |
| **Country of implementation** | United Kingdom |
| **Additional information** | https://www.thinkuknow.co.uk/professionals/resources/thinkuknow-toolkit/<br>https://www.src.ac.uk/images/news/658x300/1920/Aug19/StudAct/Thinkuknow_Toolkit.pdf |

**Table II-12: Cybercrime prevention programs/projects - THINKUKNOW - "JOSH & SUE"**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | Young people with learning disabilities aged 11-13 |
| **Themes/Problems** | Internet Security |
| **Objectives** | • Young people should be able to understand the consequences associated with inappropriate online attitudes/behaviours by exploring online safety behaviours and positive behaviours in online interpersonal relationships |
| **Implementation context** | School and/or family context |
| **Description** | • The film is available in two versions, for young people with different levels of learning disabilities.<br>• The film can be used in a school and/or family context. |
| **Country of implementation** | United Kingdom |
| **Additional information** | https://www.thinkuknow.co.uk/parents/Support-tools/Films-to-watch-with-your-children/Josh_and_Sue_original1/ |

**Table II-13: Cybercrime prevention programs/projects - ZUKY'S SAFETY GUIDE**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | Children (no age specification) |
| **Themes/Problems** | Internet Security |
| **Objectives** | • Informing children about risks on the Internet and cyber-security strategies and personal protective behaviours |
| **Implementation context** | Can be implemented in any context, by the family, carers and/or professionals |
| **Description** | • Animated series for children, where the main character is "Zuky", an Internet security superhero. This series can be viewed on the official website or on Youtube. By using the official website, besides the videos, guides and quizzes are also available for children, as well as advice for families and legal guardians on Internet safety. |
| **Country of implementation** | Netherlands |
| **Additional information** | https://www.paloaltonetworks.com/campaigns/kids-in-cybersecurity<br>https://www.youtube.com/channel/UCDYFyxEbTw0oF0FdzP1hlfg<br>https://trailhead.gsnorcal.org/wp-content/uploads/2018/12/EN_PANE_Onepaper_Kids_in_Cybersecurity.pdf |

**Table II-14: Cybercrime prevention programs/projects - PROJECT deSHAME**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | Young people aged between 13 and 17 years old |
| **Themes/Problems** | Online sexual harassment |
| **Objectives** | • Promote the reporting of sexual harassment online among young people<br>• Improve multisectorial cooperation in the prevention and response to these behaviours |
| **Implementation context** | Community and school context |
| **Description** | The deSHAME Project is funded by the European Commission and aims to combat online sexual harassment. It is a collaboration between *Childnet* (UK), *Save the Children* (Denmark), *Kek Vonal* (Hungary) and *UCLan* (UK). It involves the development of a range of educational resources to prevent sexual harassment online and to enable reporting it. Within this framework, the *Step Up, Speak Up!* toolkit was developed - a tool with hands-on sessions to address sexual harassment online among young people. Several resources and support materials were also developed for the school context. |
| **Country of implementation** | Various |
| **Additional information** | https://www.childnet.com/our-projects/project-deshame<br>https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf |

[111] The project defines online sexual harassment as a set of unwanted sexual behaviours that can occur on any digital platform. This comprehensive concept incorporates different forms of cybercrime/violence addressed in Part I, Chapter 1 of this Handbook, including *cyberbullying*, non-consensual dissemination of images and videos, and different forms of child sexual abuse and exploitation over the Internet.

**Table II-15: Cybercrime prevention programs/projects - KIDS IN THE KNOW - "ZOE & MOLLY ONLINE"**

| | |
|---|---|
| **Type of prevention** | Universal |
| **Target population** | 1st cycle students |
| **Themes/Problems** | Internet Security |
| **Objectives** | • Students should be able to identify the risks and benefits in using the Internet<br>• Students should be able to respond safely to the risks they encounter online |
| **Implementation context** | School context<br><br>It also has a website with games, quizzes and comics, which can be used in a school context, as a complement, or in a family context. |
| **Description** | • *"Zoe & Molly Online"* is a comic book. Developed by the *Canadian Centre for Child Protection*, *"Zoe & Molly Online"* is designed to promote classroom discussions about the risks associated with sharing personal information online.<br>• Promotes adult involvement and supervision by encouraging children to always check with a trusted adult before sharing information online with anyone. |
| **Country of implementation** | Canada |
| **Additional information** | http://www.zoeandmolly.ca/pdfs/zm_TeacherKit_SinglePagesGr4_en.pdf<br>https://www.zoeandmolly.ca/app/en/ |

### 4.2.1. The example of public information and awareness campaigns

The media are powerful tools for dissemination, playing a major role in preventing violence and crime in different dimensions (APAV, 2011).

The media can therefore be an important channel in the prevention of cybercrime, in particular through the dissemination of public information and awareness campaigns in this area, either through different media, including the Internet and social networks, or via more traditional ones such as television. In any case, information and awareness campaigns should be used as part of a broader approach to the prevention of cybercrime (Brewer et al., 2019).

The campaigns can have different objectives (Finn & Banach, 2000; Brewer et al., 2019), such as:

- Providing information on cybersecurity measures and personal protective behaviours for the use of the Internet and ICT;

HIGHLIGHT | PRACTICES IN FOCUS:

*The European Network and Information Security Agency* (ENISA) promotes annually the awareness campaign *European Cyber Security Month*.

This European campaign seeks to raise awareness of cybersecurity threats and to promote cybersecurity among individuals and organisations.

This campaign also provides resources on personal protection, information on a range of education initiatives and sharing of good practices.

Previous campaigns and their resources, including videos and infographics, are available at https://cybersecuritymonth.eu/press-campaign-toolbox/infographics

Full information about the *European Cyber Security Month* initiative is available at https://cybersecuritymonth.eu/

- Promote positive behaviours and values associated with the use of the Internet and ICT;

HIGHLIGHT | PRACTICES IN FOCUS:

Under the 2019 *European Cyber Security Month* campaign, the motto of cyberhygiene is used to inform and raise awareness about the importance of healthy and safe use of ICT and the Internet in everyday life.

The campaign materials can be accessed at: https://cybersecuritymonth.eu/#/campaign

The *European Cyber Security Month* campaign and the *European Network and Information Security Agency* provide a range of information and awareness promotion resources.

Among them, *Network and Information Security (NIS) QUIZ* stands out: a self-diagnostic tool that allows assessing levels of knowledge and skills on subjects such as cybersecurity in general, privacy and cybersecurity threats.

This tool, available in several languages, can be accessed and used at: https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/

- Inform about the behaviours to be adopted in cyber-victimisation situations;

HIGHLIGHT | PRACTICES IN FOCUS:

EUROPOL's Say No! public awareness campaign aims to raise awareness in children and young people so that they can identify and act on online sexual extortion of children, reinforcing the importance of reporting and seeking support.

The campaign videos (in several languages) and other information resources are available at: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime.

- Promoting collective or third-part involvement in online protection and safety (e.g. the role of the family in identifying the risk associated with their children's online behaviours);
- Dissuade against the practice of cybercrime by providing information regarding the associated risks and negative consequences.

HIGHLIGHT | PRACTICES IN FOCUS:

EUROPOL, with a distinct register and purpose, launched the *Cyber crime vs. cyber security: what will you choose?* awareness campaign

Available in different languages, this campaign is also aimed at young people and aims to deter them from engaging in cybercrime by highlighting the consequences and costs associated with engaging in these illicit behaviours.

The campaign material is available for download at: https://www.europol.europa.eu/publications-documents/cyber-crime-vs-cyber-security-what-will-you-choose-poster

Under the initiative, EUROPOL also provides information and advice for young people as well as for educators and families.

## 4.3. The family's role in prevention

Current adults, unlike children and young people, were not born 'digital natives', so they don't accept so promptly the Internet and ICT as something natural, fundamental and unquestionable in their life. In addition, besides their effective and efficient use of the Internet and ICT being constrained by their limited knowledge and skills, the family often does not have a clear awareness of their children and young people's online activities (Richardson & Milovidov, 2019; Cross et al., 2016; Lwin et al., 2013; Öztürk & Akcan, 2016).

Paradoxically, adults in the family play a key role in informing and educating children and young

people about a safe use of the Internet and ICT and, consequently, in the prevention of cyber-victimisation and online risk behaviours (Mesch, 2009; Notar et al., 2013; Morais, 2012 *cit in* Martins et al., 2017; Smallbone & Wortley, 2017; Richardson & Milovidov, 2019).

Family intervention is therefore very important:

- In setting up and implementing **consistent rules** for the use of the Internet and ICT by children and young people under the adults' responsibilty;
- In educating children and young people about their **rights and responsibilities** when using the Internet and ICT;
- In **promoting empathy** and respect for others in any context, including online;
- In providing **information** and empowering children and young people on issues of privacy, cybersecurity and personal protection when using the internet and ICT, as well as clearly **presenting the risks** associated with the use of the internet and ICT, including those related to violence and crime;
- In **monitoring the use of the Internet and ICT**, through open communication, learning to use the Internet and ICT, and interest in online activities by the children and young people under the family's responsibility;
- Identifying possible **indicators of cyber-victimisation** (or unhealthy use of ICT and the Internet) on the children and young people, and enabling appropriate intervention/protection of the child or young person in cybercrime situations;
- Maintaining **communication channels** with children and young people in order to promote looking for support/help from trusted adults in situations of cyber-victimisation and other circumstances in which personal protection on the Internet and ICT may be compromised.

HIGHLIGHT | PRACTICES IN FOCUS:

*INTERNETMATTERS.ORG* is a non-profit organisation that aims to empower families to keep children and young people safe when using the Internet and ICT.

The platform has information, advice and several specific resources for families with children and young people of different age groups.

It also has information on different types of cybercrime that can affect children and young people, such as online grooming, cyberbullying, online identity theft, among others.

The platform is available at: https://www.internetmatters.org/

*PARENTINFO.ORG* is also a platform aimed at parents and families, with information and advice on a range of topics of interest related to the Internet and ICT, including issues such as cybersecurity, applications and technology, well-being and health, among others.

The platform is available at: https://parentinfo.org/

Still with regard to the role of the family in cybercrime prevention, the concept of *digital parenting* was introduced and can be operationalised as:

- Open communication between the family/parents and the children and young people under their responsibility;
- Family/parents involvement on online activities carried out by children and young people, in the same way that they are involved in children and young people's daily activities in *traditional* contexts;
- Protecting the children and young people's digital presence, i.e. the way the child or young person presents or portrays themselves in their online activities;
- Mutual learning between the family/parents and the children and young under their responsibility;
- Protecting dependent children and young people from the Internet and ICT risks and threats, particularly cybercrime.

HIGHLIGHT | PRACTICES IN FOCUS:

The Council of Europe launched *Parenting in the Digital Age Parental guidance for the online protection of children from sexual exploitation and sexual abuse*.

It is a good practice guide for parents and families, in which different forms of child sexual abuse and exploitation via the Internet are addressed. In a practical and informative way, this guide shares tips and resources aimed at helping parents and families to protect children and young people from these phenomena and even to act in situations where cyber-victimisation has already occurred.

The guide is available at https://rm.coe.int/digital-parenting-/16807670e8

The Council of Europe also makes available a number of other information and educational resources concerning the protection of children and young people on the Internet. For example, the Council of Europe's *Internet Literacy Handbook*, also available for download at: https://www.coe.int/en/web/children/internet-literacy-handbook.

See also https://www.coe.int/en/web/children/the-digital-environment for additional information..

## 4.4. The school as a privileged prevention context

School, alongside the family, is a **very important socialising context** for the development of children and young people, not only in terms of curricular learning, but also in terms of learning **social skills for life**. These are fundamental skills for the child or young person's functioning and behaviour in relation to the world around them (Saavedra & Machado, 2010), particularly in their closest relational contexts, such as the peer group and the family, but also to their functioning in society. The quality of the bond between the child or young person and the school is also a protective factor against risk behaviours, which is why it is particularly important to promote opportunities, in a school context, for

strengthening the well-being and positive relationships of children and young people with their peers and education professionals (McNeely, Nonnemaker, & Blum, 2002 cit *in Saavedra* & Machado 2010). School is thus a natural context for the implementation of crime and violence prevention initiatives, since most children attend school and "live" *in* that context a significant part of their time (Durlak, 1995 *cit in idem*).

The table below presents a set of desirable characteristics for the effectiveness of prevention programs in the school context (APAV, 2011; Brewer et al., 2019):

**Table II-16: Main aspects to be considered in school-based prevention programmes**

| |
|---|
| **Coherent theoretical basis:** the starting point for planning should be a clear theoretical basis with evidence of success provided by research. |
| **Ecological approach:** the programme should focus not only on the individual but also on their social contexts: family, school, community. School intervention programmes are most successful when complemented by family and community interventions, as these can reinforce and promote behaviour change. |
| **Integrated approach to risk and protective factors:** programmes should be developed in a way that reduces risk factors and promotes protective factors. |
| **Individualized attention:** the intervention should be planned according to the specific needs of the individual/group; programmes should be appropriate to the age, level of development and characteristics of the target groups. |
| **Early and developmentally adjusted intervention:** intervention should take place as early as possible, according to the level of development of individuals. |
| **Choosing the right targets for change:** increasing knowledge, changing attitudes, changing behaviours and learning new skills are the most common targets for change. |
| **Peer involvement:** given the influence of peers, there are prevention programmes based on the action of peer groups as preventive agents. |
| **Use of interactive methods of transmitting information:** activities should be carried out in an interactive, appealing and age-appropriate format: discussion groups, debates, brainstorming, role-play, etc. |
| **Systematic learning and skills training:** opportunities should be provided for social skills training: conflict resolution, assertiveness, decision making, active listening, as well as training through cognitive-behavioural strategies such as role-play, simulation of situations close to reality and the participants' personal experiences, etc. |
| **Promotion of social consciousness:** prevention programs should help recipients understand the emotions and thoughts of others [empathy] and appreciate positive interaction with different groups. |
| **Emotional management:** prevention programs should help participants to deal adequately and efficiently with emotions [emotional self-management]. |
| **Focus on relationships:** prevention programmes should prepare participants to establish positive relationships with others, promoting their ability to communicate, cooperate, negotiate solutions to conflicts, seek help [if necessary], and resist peer pressure and environmental challenges in an appropriate way. |
| **Training, supervision and multidisciplinary work:** professionals' preparation is fundamental for a quality and successful implementation. |

**Neutral gender approach:** it is important to respect the gender identity of the recipients and to consider this variable in the intervention process.

**Focus on the problems' normative levels:** besides the most serious or severe forms of violence, prevention programmes should address the 'normative' levels of violence (including subtle forms of violence that are usually tolerated or normalised by the intervention's target group).

**Behavioural alternatives:** the intervention should present behavioural alternatives in contrast with the use of inappropriate behaviour.

**Information:** programmes should also cover the provision of information about risk factors and the consequences of certain behaviour and about social support structures.

**Clear content and simple materials:** the programme should have user-friendly guides and/or manuals to support implementation.

**Full implementation of the programme:** the programmes must be implemented in their entirety and fulfilling the proposed objectives, with mechanisms for monitoring their implementation.

**Intensive and long-term intervention:** prevention programmes must be intensive and long-term.

**Evaluation:** prevention programmes should include the independent (external to the team responsible for their creation/implementation) measurement of changes achieved in the target groups using validated methodologies.

**Sustainability:** it is also important to evaluate the costs versus benefits of implementation and their long-term sustainability.

HIGHLIGHT | PRACTICES IN FOCUS:

*NoTrap!* is an Italian online and school-based intervention program designed to prevent and combat bullying and cyberbullying.

ICT is the starting point of the programme, with two basic assumptions:

- The use of ICT can increase the risk of cyberbullying.
- ICT can also be used as a tool to train and strengthen knowledge and skills in prevention and action against cyberbullying.

Evaluation studies of this programme have identified positive results in reducing bullying and cyberbullying (Palladino et al., 2016).

HIGHLIGHT | PRACTICES IN FOCUS:

The Project *CyberTraining: A Research-based Training Manual On Cyberbullying* focussed on the issue of cyberbullying, with the support of research teams from Germany (responsible for coordination), Portugal, Spain, UK, Ireland and information and communication technologies and digital culture experts from Bulgaria, Switzerland and Norway.

This project has produced a training manual on cyberbullying, aimed in particular at professionals working on this area with different target audiences, especially young people, families and schools. In addition to including a theoretical component, this manual also offers guidance, support, and resources that can be used to preventing and combating this problem (Matos et al., 2011).

## 4.5. Prevention for vulnerable groups: the case of children and young people

As ICT natives, children and young people show an **almost natural interest and appetite for online activities**. This is advantageous in many areas, but also increases **this group's vulnerability to involvement in cybercrime**, both in terms of cyber-victimisation and perpetration (Alkan & Citak, 2007 cit *in Edirisuriya* & Liyanage, 2016).

For this group, communication through Internet-supported communication tools and virtual communities are not technological subcultures, but rather ways of keeping in touch with peers. Communication through these media seems to be privileged by this population, as it provides a greater sense of privacy and anonymity, favoring disinhibition, at the expense of face-to-face communication (Chisholm, 2014).

Because they move naturally through the Internet and ICT, it is not uncommon for young people to be involved in illegal online activities, either by seeking sensations, for fun or because they do not associate possible negative consequences with their behaviour. The *PRACTICE IN FOCUS* summarised above – the EUROPOL's *Cyber crime vs cyber security: what will you choose?* awareness campaign - informs and warns about the consequences of engaging in illicit online activities and, in opposition, seeks to promote the adoption of positive and normative behaviours.

Similarly, the risk of cyber-victimisation is also higher among the younger population. See the *STATISTICS IN FOCUS* presented at various points in Part I, Chapter 1 of this Handbook.

HIGHLIGHT | PRACTICES IN FOCUS:

Following the EUROPOL's public awareness campaign on online sexual extortion mentioned above, the campaign *YOUR LIFE IS ONLINE. PROTECT IT!* offers a range of information for young people aiming at reducing the risk associated with their online behaviour and exposure levels.

It covers information on cyber security measures to be adopted and that increases the **levels of digital privacy**, particularly on social networks, and also addresses other **personal protective behaviors** that reduce the risk of cyber-victimisation.

See https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media

Additionally, *YOUR LIFE IS ONLINE. PROTECT IT!* also provides information and instructions on how to act in situations of cyber-victimisation, such as:

- How to request the removal of content on different platforms in the case of non-consensual disclosure of images and videos: https://www.europol.europa.eu/removing-links-to-explicit-content
- How to ask for help and report situations of cyber-victimisation: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/are-you-victim-get-help-report-it-we-are-here

## 4.6. Situational cybercrime prevention: a question of opportunity

**Situational crime prevention** is a theoretical paradigm that focuses on the circumstances associated with criminal opportunities and how the environment, conditions and context can be modified to prevent these criminal opportunities. This paradigm is associated with Rational Choice Theory and[112] Routine Activity Theory (Hinduja & Kooi, 2013):

- Rational choice operates at a micro level, and assumes that criminal behaviour is driven by a goal that would lead to a benefit. Thus, eventual changes in the opportunity structure may affect perceptions of risk, effort and reward.
- Routine activities operate at a macro level, demonstrating that daily life changes affect the movement of likely crime targets, the eventual offenders' likelihood of action, and levels of surveillance.

Situational crime prevention introduces the potential for change in environments where crime can occur, making these same environments less attractive to motivated offenders. Crime prevention thus relies on reducing offenders' opportunities to benefit from vulnerabilities by managing, designing and manipulating that environment, i.e. by **creating obstacles in the environment that reduce the likelihood of criminal opportunities**. Ideally, these efforts will serve to **increase the risk and effort** associated with illicit activity and to **diminish the rewards of successful crime**. If the presence and attractiveness of criminal opportunities is reduced, then the outcome will be a reduction in crime (Clarke, 1997cit *in* Hinduja & Kooi, 2013).

Over several decades, a range of proposals and specific intervention measures have been defined for environments in which crimes occur – these are called **situational prevention techniques**. Their main objective is to reduce the opportunity for crime to occur by changing environmental conditions. There are five categories of situational prevention and, in each of these categories, five specific techniques can be applied (Cornish & Clarke, 2003 cit *in* Agustina, 2015):

**Category *Increase the effort:***

If the effort to commit a particular crime has to increase, it may be possible to dissuade the perpetrator from committing it.

This category includes 5 types of techniques:

- target harden (implementation of barriers that make it difficult to access to the target);
- control access to facilities (block access to places where criminal action may occur);
- screen exists (control exits/movements in a *place*);
- deflect offenders (change the movement patterns of potential perpetrators)
- control tools (limiting access to tools that are part of the *modus operandi*).

[112] Criminological theories (and their application to the understanding of cybercrime) are addressed in Part I, Chapter 3, section 3.1 of this Handbook.

**Category *Increase the risks:***

These techniques are intended to increase the risk of the perpetrator being detected and include:

- increased protective activities/extend guardinaship (creating activities so that people feel more protected; for example, *neighbourhood watch*);
- assist natural surveillance (e.g. by increasing the visibility of a given location);
- reduce anonymity;
- informal surveillance (e.g. through increased staff movement within a trade area);
- formal surveillance (e.g. through increased policing).

**Category *Reduce the rewards:***

This category aims at reducing the rewards that potential offenders may benefit from when committing a crime.

The main techniques are:

- conceal targets (e.g. parking in a private garage, rather than in a public place/street);
- remove targets (e.g. removing electronic devices and other goods when parking the car);
- identify property (e.g. vehicle registration);
- disrupt market transactions (e.g. licensing of services and trades);
- deny benefits (e.g. using a mobile phone password).

**Category *Reduce provocation:***

This category aims to prevent triggers of criminal practice.

The main techniques are:

- reduce frustrations and stress (e.g. informing about public transport arrival/waiting time);
- avoid disputes (e.g. separating sports supporters in football/sport matches);
- reduce emotional arousal (e.g. controlling watching violence in the media);
- neutralise peer pressure (e.g. awareness campaigns);
- discourage imitation (e.g. maintaining clean spaces and quick removal of vandalism indicators).

**Category *Remove excuses*:**

It includes the following situational prevention techniques:

- set rules;
- display instructions (e.g. signs such as 'no parking');
- alert conscience (e.g. raise awareness for the behaviour being illegal);
- assist compliance (e.g. at festive events, facilitate access to public transport);
- control alcohol and drugs (e.g. imposition of a maximum number of drinks in nightlife venues).

Situational prevention approaches have been widely used in *traditional* contexts and have been proven useful in reducing different types of *traditional* crime. The relevance of situational prevention in combating cybercrime has also been analysed (Brewer et al., 2019).

In this context, Miró Llinares (2012, *cit in* Agustina, 2015) presented a combination of **concrete situational cybercrime prevention measures**:

**Table II-17: Situational prevention techniques applied to cybercrime**

| Reducing environment of incidence | Increasing perceived effort | Increasing perceived risk | Reducing perceived rewards | Eliminating excuses |
|---|---|---|---|---|
| Don't introduce targets | Control access to system | Extend guardianship/ surveillance | Hide targets | Set rules |
| Identify risk zones | Detect and impede the attack | Reducte anonymity | Remove targets | Set rules |
| Decontamination/ residue cleanup | Deflect offenders | Strengthen formal surveillance | Remove benefits | Strengthen moral conscience |
| Separatation of targets | Control tools/weapons | Assist natural surveillance | Disrupt markets | Assist compliance |

Five categories were developed - reducing environment of incidence; increasing perceived effort; increasing perceived risk; reducing perceived rewards; eliminating excuses – and they include 20 situational cybercrime prevention techniques. *Reducing environment of incidence* includes not introducing targets (e.g. no access to chats), identifying risk areas (e.g. information campaigns on risk on social networks), decontamination/residue cleaning up and separation of targets (e.g. creation of local security sub-networks). *Increasing perceived effort* includes: controlling system access (e.g. updating operating systems and passwords and licenses); detecting and preventing attacks (e.g. antivirus; anti-spyware; anti-spam); deflecting offenders (e.g. removal of illegal content; denial of access to[113] specific IPs); controlling tools/weapons. *Increasing perceived risk* covers extending guardianship/surveillance (e.g. third-part reporting), reducing anonymity (e.g. identifying

[113] IP refers to the Internet protocol address and refers to the label/code assigned to each device connected to the computer network.

IPs; registration on web forums; user identification systems), strengthening formal surveillance (e.g. specialised teams in cybercrime investigation) and assisting natural surveillance (e.g. improving IP identification systems). The fourth category focuses on: hiding targets (e.g. using encryption systems; hiding personal data on social networks); removing targets (e.g. using removable hard drives; choosing alternative payment systems such as *PayPal*; not accepting messages from unknown people); removing benefits; disrupting markets (e.g. controlling direct download websites). Finally, *eliminating excuses* includes: setting rules (e.g. international legal harmonisation); setting rules (e.g. privacy notifications on social networks); strengthening moral conscience (e.g. raising awareness for intellectual property); and assisting compliance (e.g. legal hacker competitions; strenghten open software).

The available evidence on the effectiveness of situational prevention techniques for cybercrime has been focused on increasing the effort, such as control and detection mechanisms/software, and on increasing the risk through formal surveillance tools. For example, research into the effectiveness of antivirus products in detecting and preventing malware infections reveals that most products are effective in detecting and preventing such infections (Brewer et al., 2019).

# BIBLIOGRAPHY
# WEBGRAPHY

# BIBLIOGRAPHY
# WEBGRAPHY

# BIBLIOGRAPHY


Agustina, J. R. (2015). Understanding cyber victimization: Digital architectures and the disinhibition effect. *International Journal of Cyber Criminology, 9*(1): 35-54.

Ajzen, I. (1991). The theory of planned behavior. *Organizational behavior and human decision processes, 50*(2), 179-211.

Al-Ali, A. A., Nimrat, A., & Benzaid, C. (2018). Combating Cyber Victimisation: Cybercrime Prevention. In *Cyber Criminology* (pp. 325-339). Springer, Cham.

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of *ciber--stalking* among college students. *Brief treatment and crisis intervention*, 5(3), 279.

Amador, N. J. R. (2012). *Cibercrime em Portugal: Trajetórias e Perspetivas de Futuro* (Doctoral dissertation).

Ang, R. P. (2015). Adolescent *ciber-bullying*: A review of characteristics, prevention and intervention strategies. *Aggression and violent behavior, 25*, 35-42.

APAV (2011). *Manual crianças e jovens vítimas de violência: compreender, intervir e prevenir.* ISBN 978-972-8852-50-4. Lisboa: APAV.

APAV (2013). *Manual Unisexo – para o atendimento a vítimas adultas de violência sexual.* Lisboa: APAV.

APAV (2017). *T@LK Handbook – Online Support for Victims of Crime.* ISBN 978-972-8852-90-0. Lisboa: APAV.

APAV (2018). *Manual ódio nunca mais: apoio a vítimas de crimes de ódio.* ISBN 978-972-8852-91-7. Lisboa: APAV.

APAV (2019). *Manual CARE: apoio a crianças e jovens vítimas de violência sexual* (2ª edição revista e aumentada). ISBN 978-972-8852-96-2. Lisboa: APAV.

APAV (2019b). *Manual EMAV : atendimento e encaminhamento de vítimas de violência doméstica e de género : procedimentos & roteiro de recursos*. ISBN 978-989-54322-2-6. Lisboa: APAV.

Arafa, A. E., Mahmoud, O. E., & Senosy, S. A. (2015). The emotional impacts of different forms of *ciber-bullying* victimization in Egyptian university students. Egypt. J. Med. Sci, 36(2), 867-80.

Askerniya, I. How best to protect the user-individuals in Moscow from cyber crime attacks.

Balkin, J., Grimmelmann, J., Katz, E., Kozlovski, N., Wagman, S., & Zarsky, T. (Eds.). (2007). *Cybercrime: digital cops in a networked environment* (Vol. 4). NYU Press.

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. Information & management, 51(1), 138-151.

Berelowitz, S., Firmin, C., Edwards, G., & Gulyurtlu, S. (2012). I thought I was the only one. The only one in the world. *The Office of the Children's Commissioner's Inquiry into Child Sexual Exploitation In Gangs and Groups: Interim report. London: The Office of the Children's Commissioner in England.*

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022-1035.

Bossler, A. M., & Burruss, G. W. (2012). The general theory of crime and computer hacking: Low self-control hackers? In Cyber Crime: Concepts, Methodologies, Tools and Applications (pp. 1499-1527). IGI Global.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime Prevention: Theory and Applications.* Springer Nature.

Brown, C. F., Demaray, M. K., Tennant, J. E., & Jenkins, L. N. (2017). Cyber victimization in high school: Measurement, overlap with face-to-face victimization, and associations with social–emotional outcomes. *School psychology review, 46*(3), 288-303.

Buchanan, T., Paine, C., Joinson, A. N., & Reips, U. D. (2007). Development of measures of *online* privacy concern and protection for use on the Internet. *Journal of the American society for information science and technology, 58*(2), 157-165.

Burns, S., & Roberts, L. (2013). Applying the theory of planned behaviour to predicting online safety behaviour. *Crime Prevention and Community Safety, 15*(1), 48-64.

Callahan, A., & Inckle, K. (2012). Cybertherapy or psychobabble? A mixed methods study of online emotional support. *British Journal of Guidance & Counselling, 40*(3), 261-278.

Cardoso, J., Ramos, C., Almeida, T., Gomes, A., Fernandes, A., & Ribeiro, R. (2018). 117 Cyber pornography use inventory-9: factor structure and psychometric properties in the Portuguese population. The Journal of Sexual Medicine, 15(7), S177.

Chisholm, J. F. (2014). Review of the status of ciber-bullying and ciber-bullying prevention. *Journal of Information Systems Education, 25*(1), 77.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime prevention studies, 16*, 41-96.

Councill, B., & Heineman, G. T. (2001). Definition of a software component and its elements. Component-based software engineering: putting the pieces together, 5-19.

Cross, C., Richards, K., & Smith, R. G. (2016). Improving responses to *online* fraud victims: An examination of reporting and support.

Cross, D., Shaw, T., Hadwen, K., Cardoso, P., Slee, P., Roberts, C., & Barnes, A. (2016). Longitudinal impact of the Cyber Friendly Schools program on adolescents' *ciber-bullying* behavior. *Aggressive behavior, 42*(2), 166-180.

Das, S., & Nayak, T. (2013). Impact of cyber crime: Issues and challenges. International journal of engineering sciences & Emerging technologies, 6(2), 142-153.

Dashora, K. (2011). Cyber crime in the society: Problems and preventions. *Journal of Alternative Perspectives in the social sciences, 3*(1), 240-259.

# BIBLIOGRAPHY


Davies, E. L., Clark, J., & Roden, A. L. (2016). Self-Reports of Adverse Health Effects Associated with *Ciber-stalking* and Cyberharassment: A Thematic Analysis of Victims' Lived Experiences.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., & Hardyns, W. (2020). Help, I need somebody: examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior*, 106310.

De Vignemont, F., & Singer, T. (2006). The empathic brain: how, when and why?. *Trends in cognitive sciences, 10*(10), 435-441.

Dooley, J. J., Gradinger, P., Strohmeier, D., Cross, D., & Spiel, C. (2010). Cyber-victimisation: The association between help-seeking behaviours and self-reported emotional symptoms in Australia and Austria. *Journal of Psychologists and Counsellors in Schools, 20*(2), 194-209.

ECPAT, I. (2018). Towards a global indicator: on unidentified victims in child sexual exploitation material. Ecpat International: Bangkok, Thailand.

Edirisuriya, M. A. V. S., & Liyanage, L. S. (2016). Application of Protective Motivation Theory in cyber safety context: Human factor in risk mitigation.

EU Commission. (2015). Special Eurobarometer 423: Cyber Security Report.

EUROPOL (2019). Internet organised crime threat assessment (IOCTA) 2019.

Finn, J., & Banach, M. (2000). Victimization online: The downside of seeking human services for women on the Internet. *CyberPsychology & Behavior, 3*(5), 785-796.

Gañán, C. H., Ciere, M., & van Eeten, M. (2017, October). Beyond the pretty penny: the Economic Impact of Cybercrime. In Proceedings of the 2017 New Security Paradigms Workshop (pp. 35-45).

Gao, J., Li, L., Kong, P., Bissyandé, T. F., & Klein, J. (2019, February). Should you consider adware as malware in your study? In 2019 IEEE 26th International Conference on Software Analysis, Evolution and Reengineering (SANER) (pp. 604-608). IEEE.

Goucher, W. (2010). Being a cybercrime victim. Computer Fraud & Security, 2010(10), 16-18.

Grabosky, P. (2007). Requirements of prosecution services to deal with cyber crime. *Crime, law and social change, 47*(4-5), 201-223.

Greijer, S., & Doek, J. (2016). Terminology guidelines for the protection of children from sexual exploitation and sexual abuse. Luxembourg: ECPAT International.

Hansen, J. V., Lowry, P. B., Meservy, R. D., & McDonald, D. M. (2007). Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems, 43(4), 1362-1374.

Hinduja, S., & Kooi, B. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. *Security journal, 26*(4), 383-402.

Holt, T. J., & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Holt, T. J., & Bossler, A. M. (2015). Cybercrime in progress: *Theory and prevention of technology-enabled offenses*. Routledge.

Jäger, T., Amado, J., Matos, A., & Pessoa, T. (2010). Analysis of experts' and trainers' views on *ciber-bullying. Journal of Psychologists and Counsellors in Schools, 20*(2), 169-181.

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In Cyber Crime and Cyber Terrorism Investigator's Handbook (pp. 149-164). Syngress.

Jansen, J. & Leukfeldt, R. (2018). Coping with cybercrime victimization: an exploratory study into impact and change. Journal of Qualitative Criminal Justice and Criminology, 2: 205-227.

Kaakinen, M., Keipi, T., Räsänen, P., & Oksanen, A. (2018). Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 129-137.

Kanayamaa, T. (2017). Impact of Cybercrime in Japan - Findings of Cybercrime Victimization Survey. Sociology, 7(6), 331-340.

Kaniasty, K., & Norris, F. H. (1992). Social support and victims of crime: Matching event, support, and outcome. *American journal of community psychology, 20*(2), 211-241.

Kansagra, D., Kumhar, M., & Jha, D. (2016). Ransomware: A Threat to Cyber security. CS Journals, 7(1).

Kienzle, D. M., & Elder, M. C. (2003, October). Recent worms: a survey and trends. In Proceedings of the 2003 ACM workshop on Rapid malcode (pp. 1-10).

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470-486.

Koops, B. J. (2010). The internet and its opportunities for cybercrime. Transnational Criminology Manual, M. Herzog-Evans, ed., 1, 735-754.

Kratchman, S., Smith, J. L., & Smith, M. (2008). The Perpetration and Prevention of Cybercrimes. Available at SSRN 1123743.

LaRose, R., & Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and *online* privacy behavior. *Journal of Consumer Affairs*, 41(1), 127-149.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: a model of *online* protection behaviour. *Behaviour & Information Technology, 27*(5), 445-454.

Leukfeldt, E. R. (2015). Organised cybercrime and social opportunity structures: A proposal for future research directions. The European Review of Organised Crime, 2(2), 91-103.

# BIBLIOGRAPHY


Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. Victims & Offenders, 15(1), 60-77.

Ljungwald, C., & Svensson, K. (2007). Crime Victims and the Social Services: Social Workers' Viewpoint. *Journal of Scandinavian Studies in Criminology and Crime Prevention, 8*(2), 138-156.

Louderback, E. R., & Antonaccio, O. (2017). Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: The role of thoughtfully reflective decision-making. Journal of research in crime and delinquency, 54(5), 639-679.

Lwin, M. O., Ang, R. P., & Liu, C. (2013). Cognitive, personality, and social factors associated with adolescents' *online* personal information disclosure.

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of adolescence, 35*(1), 31-41.

Maia, R. L., Nunes, L. M., Caridade, S., Sani, A. I., Estrada, R., Nogueira, C., Fernandes, H. & Afonso, L. (2016). *Dicionário - Crime, Justiça e Sociedade* (1.ª ed.). Lisboa: Edições Sílabo.

Maimon, D., & Louderback, E. R. (2019). Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2:191-216.

Mallen, M. J., Vogel, D. L., & Rochlen, A. B. (2005). The practical aspects of *online* counseling: Ethics, training, technology, and competency. *The Counseling Psychologist, 33*(6), 776-818.

Maran, D. A., & Begotti, T. (2019). Prevalence of *Ciber-stalking* and Previous *Offline* Victimization in a Sample of Italian University Students. Social Sciences, 8(1).

Marcum, C. D., Higgins, G. E., Ricketts, M. L., & Wolfe, S. E. (2014). Hacking in high school: Cybercrime perpetration by juveniles. Deviant Behavior, 35(7), 581-591.

Marczak, M., & Coyne, I. (2010). *Ciber-bullying* at school: Good practice and legal aspects in the United Kingdom. *Journal of Psychologists and Counsellors in Schools, 20*(2), 182-193.

Marques, P. P. L. D. C. (2013). *Informática forense: recolha e preservação da prova digital* (Doctoral dissertation).

Martellozzo, E., & Jane, E. A. (Eds.). (2017). Cybercrime and its victims. Taylor & Francis.

Martins, M. J. D., Simão, A. M. V., Freire, I., Caetano, A. P., & Matos, A. (2017). Cyber-victimization and cyber-aggression among Portuguese adolescents: The relation to family support and family rules. In *Violence and society: Breakthroughs in research and practice* (pp. 134-149). IGI Global.

Matos, A., Pessoa, T., Amado, J., & Jäger, T. (2011). Agir contra o *ciber-bullying*–manual de formação. *Literacia, Media e Cidadania*, 183-196.

McCann, I. L., & Pearlman, L. A. (1990). Vicarious traumatization: A framework for understanding the psychological effects of working with victims. *Journal of Traumatic Stress, 3*(1), 131–149.

McGonagle, T. (2013). The Council of Europe against online hate speech: Conundrums and challenges. In Expert paper. Belgrade: Council of Europe Conference of Ministers responsible for Media and Information Society.

McNeeley, S. (2015). Lifestyle-routine activities and crime events. Journal of Contemporary Criminal Justice, 31(1), 30-52.

Mesch, G. S. (2009). Parental mediation, online activities, and *ciber-bullying. CyberPsychology & Behavior, 12*(4), 387-393.

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy, 13*(5), 99-103.

Moitra, S. D. (2004). Cybercrime: Towards an assessment of its nature and impact. International Journal of Comparative and Applied Criminal Justice, 28(2), 105-123.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: a multi-nation study. Journal of Scandinavian Studies in Criminology and Crime Prevention, 16(2), 203-210.

Neghina, D. E., & Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. International journal of computers communications & control, 8(1), 97-104.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology, 5(1).

Notar, C. E., Padgett, S., & Roden, J. (2013). *Ciber-bullying*: Resources for Intervention and Prevention. *Universal Journal of Educational Research, 1*(3), 133-145.

Nykodym, N., Taylor, R., & Vilela, J. (2005). Criminal profiling and insider cyber crime. Computer Law & Security Review, 21(5), 408-414.

Overvest, B., & Straathof, B. (2015). What drives cybercrime? Empirical evidence from DDoS attacks (No. 306. rdf). CPB Netherlands Bureau for Economic Policy Analysis.

Öztürk, E., & Akcan, G. (2016). Preventing and Coping Strategies for Cyber Bullying and Cyber Victimization. *International Journal of Information and Communication Engineering, 10*(5), 1771-1774.

Palladino, B. E., Nocentini, A., & Menesini, E. (2016). Evidence-based intervention against bullying and *ciber-bullying*: Evaluation of the NoTrap! program in two independent trials. *Aggressive behavior, 42*(2), 194-206.

Patel, R. D., & Singh, D. K. (2013). Credit card fraud detection & prevention of fraud using genetic algorithm. International Journal of Soft Computing and Engineering, 2(6), 292-294.

Pessoa, T., da Mota Matos, A. P., Amado, J., & Jäger, T. (2011). *Ciber-bullying*: do diagnóstico de necessidades à construção de um manual de formação. *Pedagogía social: revista interuniversitaria*, (18), 57-70.

# BIBLIOGRAPHY


Peterson, J., & Densley, J. (2017). Cyber violence: What do we know and where do we go from here? Aggression and violent behavior, 34, 193-200.

Phillips, E. (2015). Empirical Assessment of Lifestyle-Routine Activity and Social Learning Theory on Cybercrime Offending.

Poong, Y., Zaman, K. U., & Talha, M. (2006, August). E-commerce today and tomorrow: a truly generalized and active framework for the definition of electronic commerce. In Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet (pp. 553-557).

Poulin, F., Nadeau, K., & Scaramella, L. V. (2012). The role of parents in young adolescents' competence with peers: An observational study of advice giving and intrusiveness. *Merrill-Palmer Quarterly (1982-)*, 437-462.

Rathi, M., & Pareek, V. (2013). Spam mail detection through data mining-A comparative performance analysis. International Journal of Modern Education and Computer Science, 5(12), 31.

Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7: 1-15.

Reyns, B. W. (2010). A situational crime prevention approach to *ciber-stalking* victimization: Preventive tactics for Internet users and *online* place managers. *Crime Prevention and Community Safety, 12*(2), 99-118.

Reyns, B. W., & Henson, B. (2016). The thief with a thousand faces and the victim with none: Identifying determinants for *online* identity theft victimization with routine activity theory. *International journal of offender therapy and comparative criminology, 6*0(10), 1119-1139.

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime *online*: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety, 18*(1), 38-59.

Ribeiro, M. D. C. F. (2015). *Cibercrime e Prova Digital* (Doctoral dissertation).

Richardson, J., & Milovidov, E. (2019). *Digital citizenship education handbook: Being online, well-being online, and rights online*. Council of Europe.

Saavedra, R. & Machado, C. (2010). Pevenção universal da violência em contexto escolar. In C. Machado (Coord.), *Vitimologia: das novas abordagens teóricas às novas práticas de intervenção* (pp. 137-167). Braga: Psiquilíbrios Edições.

Saban, K. A., McGivern, E., & Saykiewicz, J. N. (2002). A critical look at the impact of cybercrime on consumer Internet behavior. Journal of Marketing Theory and Practice, 10(2), 29-37.

Sampson, R., Eck, J. E., & Dunham, J. (2010). Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure. *Security Journal, 23*(1), 37-51.

Santos, A. F. C. (2016). *O cibercrime: desafios e respostas do direito* (Doctoral dissertation).

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change, 102*, 320-330.

Seifert, C., Stokes, J., Lu, L., Heckerman, D., Colcernian, C., Parthasarathy, S., & Santhanam, N. (2015). U.S. Patent No. 9,130,988. Washington, DC: U.S. Patent and Trademark Office.

Sharpe, J., & Self, R. (2015). Computers for Everyone. Computers for Everyone, 1(1).

Sigurjonsdottir, S. (2013). Consequences of victims' mental health after Internet--initiated sexual abuse; a sexual grooming case in Sweden.

Skorodumov, B. I., Skorodumova, O. B., & Matronina, L. F. (2015). Research of human factors in information security. *Modern Applied Science, 9*(5), 287.

Smallbone, S., & Wortley, R. (2017). 8 Preventing Child Sexual Abuse *Online. Online Risk to Children: Impact, Protection and Prevention*, 143.

Smith, A. D. (2004). Cybercriminal impacts on online business and consumer confidence. *Online* Information Review, 28(3), 224-234.

Suler, J. (2004). The *online* disinhibition effect. CyberPsychology & Behavior, 3: 321-326.

Tanrikulu, I. (2018). *Ciber-bullying* prevention and intervention programs in schools: A systematic review. *School psychology international, 39*(1), 74-91.

van der Wagen, W., & Pieters, W. (2018). The hybrid victim: Re-conceptualizing high-tech cyber victimization through actor-network theory. *European Journal of Criminology,* 1477370818812016.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8*(2), 115-127.

Van Wilsem, J. (2013). Hacking and harassment—do they have something in common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice, 29*(4), 437-453.

Wedlock, E., & Tapley, J. D. (2016). What works in supporting victims of crime: A rapid evidence assessment.

Winkel, F. W. (1991). Police, victims, and crime prevention: Some research-based recommendations on victim-orientated interventions. *The British Journal of Criminology, 31*(3), 250-265.

Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2010). *Online* "predators" and their victims: Myths, realities, and implications for prevention and treatment.

World Health Organization. (2017). Responding to children and adolescents who have been sexually abused: WHO clinical guidelines. ISBN 978-92-4-155014-7. Geneva: World Health Organization.

Wright, J. (2002). *Online* counselling: Learning from writing therapy. *British Journal of Guidance and Counselling, 30*(3), 285-298.

Wright, M. F. (2015). Cyber Victimization: A New Kind of Victimization. *Nova Science Publishers, Inc.*

Wright, M. F. (2018). Ciber-stalking victimization, depression, and academic performance: The role of perceived social support from parents. *Cyberpsychology, Behavior, and Social Networking, 21*(2), 110-116.

Yar, M. & Steinmetz, K. F. (2019). Cybercrime and society (3rd edition). ISBN 978-1-5264-4065-5. London: SAGE.

Yucedal, B. (2010). Victimization in cyberspace: An application of Routine Activity and Lifestyle Exposure theories (Doctoral dissertation, Kent State University).

# WEBGRAPHY


http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis

https://apav.pt/cibercrime/

https://articles.forensicfocus.com/2019/12/17/investigating-nonconsensual-intimate-image-sharing/

https://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-COR-1-DCL-1/en/pdf

https://dre.pt/legislacao-consolidada/-/lc/34520775/view

https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf

https://techterms.com/definition/hardware

https://www.cncs.gov.pt/recursos/glossario/

https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html

https://www.gesetze-im-internet.de/tkg_2004/

https://www.gesetze-im-internet.de/tmg/BJNR017910007.html

https://www.innocentlivesfoundation.org/gaming-and-grooming-how-minecraft-and-fortnite-could-be-dangerous/

https://www.kaspersky.com/blog/online-dating-report/

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/online-shopping/

https://www.scamwatch.gov.au/types-of-scams/dating-romance

ROAR
empoderamento às vítimas de cibercrime

APAV
associação portuguesa de Apoio à Vítima

This Manual was funded by the European Union's Internal Security Fund– Police

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

WEISSER RING
Wir helfen Kriminalitätsopfern.

ACTEDO

altice



ISBN:
978-989-54855-8-1