Manual ROAR

–

de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitarea victimelor

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

Promotor:
Associação Portuguesa de Apoio à Vítima (APAV) | Portugalia

Parteneri:
Ministério da Administração Interna (MAI) | Portugalia
Procuradoria-Geral da República (PGR) | Portugalia
PT Portugal | Portugalia
Weisser Ring | Germania
Centrul de Acțiune pentru Egalitate și Drepturile Omului (ACTEDO) | România

ISBN: 978-989-53116-2-0
Descriere CIP:

Titlu:
Manual ROAR - de la înțelegerea și prevenirea criminalității informatice la sprijinirea și capacitarea victimelor

Adresă:
APAV – Associação Portuguesa de Apoio à Vítima
Rua José Estêvão, 135 A
1150-201 Lisabona
Portugalia

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

CUPRINS

CUPRINS

PARTEA I
SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

PARTEA I

SĂ ÎNȚELEGEM CRIMINALITATEA INFORMATICĂ

1. CRIMINALITATEA INFORMATICĂ: O ABORDARE CONCEPTUALĂ

1.1. Tehnologiile informației și comunicațiilor (TIC) și apariția criminalității informatice

IMPORTANT | STATISTICI ÎN FOCUS:

Potrivit EUROSTAT[1], în 2017, 87% din gospodăriile din Uniunea Europeană aveau acces la Internet, comparativ cu 70% în 2010.

Peste 85% dintre persoanele chestionate au raportat că folosesc zilnic internetul. Cele mai mari cote de utilizare au fost identificate în Italia, Danemarca, Malta, Olanda și Suedia.

EUROSTAT a analizat, de asemenea, utilizarea internetului de către companii și organizații: doar 3% dintre companiile din Uniunea Europeană nu aveau internet în 2017, iar cele mai mari proporții de neutilizare s-au găsit în România și Grecia.

În același sondaj, EUROSTAT a măsurat câțiva indicatori de comerț electronic: în ultimii 10 ani, cumpărăturile online au crescut pentru utilizatorii de internet de toate vârstele, cu accent deosebit pe tinerii cu vârste cuprinse între 16 și 24 de ani. De asemenea, sondajul adresat întreprinderilor și organizațiilor a raportat că 20% dintre companii au efectuat comerț electronic în 2017.

Datele de mai sus (și alte surse) arată utilizarea tot mai sporită a internetului, în special în Uniunea Europeană, la diferite niveluri. Acestea reiterează, de asemenea, că Internetul este într-adevăr și din ce în ce mai global, instantaneu, intrinsec transfrontalier, oferind o structură de rețea descentralizată și permițând prezentarea digitală a informațiilor (Koops, 2010).

Internetul și tehnologiile informației și comunicațiilor (TIC) au facilitat, de asemenea, datorită acestor caracteristici similare, oportunități variate de criminalitate, modificând și crescând posibilitățile de criminalitate, fie pentru că sunt în sine potențiale ținte ale criminalității, fie pentru că pot oferi, de asemenea, mijloacele sau instrumentele prin care pot fi comise alte infracțiuni (Van Wilsem, 2011).

Prin urmare, se poate spune că Internetul a oferit **noi forme și oportunități de a ofensa sau comite infracțiuni care pot fi desemnate drept „convenționale"**, cum ar fi urmărirea, abuzul sexual al copiilor sau frauda, dar a valorificat și **apariția unor noi forme de infracțiuni** asociate exclusiv cu utilizarea computerelor, TIC și sisteme informatice, cum ar fi hacking, DDoS și malware, care vor fi detaliate în următoarele secțiuni ale acestui manual (Yucedal, 2010; Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

Mai detaliat, resursele furnizate de Internet, privite ca „chei transformatoare", au **revoluționat modul în care poate fi comisă o infracțiune** (Wall, 2007 cit în Jahankhani și colab., 2014). Ne referim la următoarele funcții promovate sau activate de Internet:

- **Globalizare**: spațiul informatic oferă noi oportunități de a depăși limitele convenționale;

[1] *Economia și societatea digitală în UE - O plimbare prin lumea noastră online în cifre | Ediția 2018*, disponibilă la https://ec.europa.eu/eurostat/cache/infographs/ict/index.html.

- **Rețele distribuite**: generează noi oportunități de victimizare;
- **Sinopticism și panopticism**: ele consolidează posibilitatea ca potențialele victime să poată fi monitorizate online;
- **Trasee de date**: creează noi oportunități de a comite criminalitatea informatică.

Mai mult, Internetul a condus la apariția unui set de medii online în care poate avea loc criminalitatea informatică. Acestea sunt:

- **Web-ul de suprafață** (site-uri web și computere accesibile și conectate la Internet);
- **Deep web** (site-uri web care nu pot fi căutate pe suprafața web; intranet și baze de date medicale);
- **Dark Web-ul** (subset al deep web-ului care constituie o platformă atractivă pentru inițierea și dezvoltarea activităților ilegale).

(Maimon & Louderback, 2019).

În acest „ecosistem", putem identifica interacțiunea următorilor agenți sau actori, al căror comportament respectiv poate duce la criminalitatea informatică:

- **Infractor informatic**;
- **Sprijinitori** - cei care susțin activitățile ilegitime ale criminalității informatice, cum ar fi programatorii și dezvoltatorii[2] care dezvoltă software[3] rău intenționat (malware[4]), distribuitorii și furnizorii care vând / furnizează instrumente care permit practicarea criminalității informatice.
- **Ținte**;
- **Gardieni** - autorități de poliție și administratori de sistem.

1.2. De la definițiile criminalității informatice la tipologii

În această secțiune a manualului prezentăm posibile definiții pentru conceptul de criminalitate informatică și, pentru o mai bună înțelegere a acestui fenomen, folosim, de asemenea, diferite tipologii și categorii pentru a demonstra complexitatea acesteia și gama de forme sau tipuri de acte incluse.

Conceptul de **criminalitate informatică** a fost desemnat inițial drept „infracțiune informatică" și acoperea toate infracțiunile care utilizează computere sau alte dispozitive similare, inclusiv rețele și alte mijloace de acces. S-au referit, prin urmare, la tot felul de **atacuri împotriva disponibilității, integrității și confidențialității sistemelor informatice, a sistemelor informaționale și a resurselor care le susțin** (hardware[5]) (Gouveia, 2016 cit în Maia, Nunes, Caridade, Sani, Estrada, Nogueira, Fernandes & Afonso, 2016).

Utilizarea tot mai mare a internetului și a TIC a accelerat apariția altor infracțiuni informatice care depășesc atacul menționat anterior asupra disponibilității, integrității și confidențialității sistemelor informatice.

[2] Dezvoltatorii sunt persoane dedicate producerii codului, testării acestuia și executării acestuia pe un server.

[3] Software-ul se referă la secvențe de instrucțiuni abstracte ale unui program, care descriu calculele care trebuie efectuate pe un dispozitiv de calcul (Councill & Heineman, 2001).

[4] Programele malware se referă la software-ul rău intenționat conceput pentru a se infiltra în mod ilicit în sistemele informatice ale altor persoane, pentru a provoca daune, modificări și / sau utilizarea incorectă a informațiilor / datelor (confidențiale sau de altă natură).

[5] Părțile *hardware* interne ale unui computer sunt denumite de obicei componente (hard disk-uri și RAM), în timp ce dispozitivele hardware externe sunt denumite de obicei periferice (monitoare, tastaturi, imprimante și scanere).

1. CRIMINALITATEA INFORMATICĂ: O ABORDARE CONCEPTUALĂ

Acest lucru duce la adoptarea unor concepte similare criminalității informatice, cum ar fi cybercrime (criminalitatea informatică), criminalitatea electronică, criminalitatea digitală și criminalitatea online.

Din această perspectivă mai largă, criminalitatea informatică poate fi definită și ca o **infracțiune în care rețeaua de calculatoare este o țintă sau un instrument *substanțial*** (Koops, 2010). În conformitate cu definiția Comisiei Europene (2007)[6], criminalitatea informatică include infracțiunile comise folosind rețele de comunicații electronice și sisteme de informații și infracțiuni împotriva acestor rețele și sisteme.

Având în vedere natura criminalității informatice și complexitatea acestui concept, mai mulți autori propun tipologii sau categorizări pentru a înțelege mai bine domeniul de aplicare al acesteia și multiplicitatea fenomenelor asociate.

Criminalitatea informatică poate fi astfel clasificată în:

- **Infracțiuni informatice dependente** - asociate cu noi forme de criminalitate, a căror apariție depinde de existența și utilizarea TIC, calculatoare și rețele de calculatoare (Leukfeldt, Notté & Malsch, 2020; Maimon și Louderback, 2019).

- **Infracțiuni facilitate informatic** - forme tradiționale de infracțiuni în care TIC joacă un rol important, include infracțiuni motivate financiar, dar și forme de violență interpersonală și infracțiuni sexuale. Exemple sunt *cyberstalking-ul* sau escrocheriile pe Internet (Leukfeldt și colab., 2020), pe care le vom aborda mai jos.

Această clasificare a criminalității informatice distinge infracțiunile informatice dependente de infracțiunile făcute posibile de internet și TIC. În acest din urmă caz, diferitele forme de criminalitate informatică care sunt făcute posibile sau activate de Internet și TIC pot fi la rândul lor subdivizate în:

- Criminalitatea informatică motivată financiar (de exemplu escrocherii de phishing[7] și bazate pe romantism[8]);
- Infracțiuni informatice în relațiile interumane (de exemplu, cyberstalking);
- Criminalitatea informatică sexuală (de exemplu, publicarea de imagini intime cu scopul răzbunării[9]).

La clasificarea de mai sus, pot fi adăugate altele, precum cele rezumate în tabelul următor.

[6] Consultați Comunicarea Comisiei către Parlamentul European, Consiliu și Comitetul Regiunilor: Către o politică generală privind lupta împotriva criminalității informatice, disponibilă la adresa https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14560&from=PT.

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

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

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

1. CRIMINALITATEA INFORMATICĂ: O ABORDARE CONCEPTUALĂ

Tabel 1: Tipuri și categorii de infracțiuni informatice

Wall, 2005 *cit in* Reep-van den Bergh & Junger, 2018	**Infracțiuni împotriva computerelor**: se referă la accesul neautorizat la granițele sistemelor informatice, cum ar fi hackingul / cracarea, unde computerele sunt punctul central / ținta atacului (de exemplu, viruși de computer); **Infracțiuni care utilizează computere**: în cazul în care TIC sunt utilizate pentru a comite infracțiuni (de exemplu, furt de identitate și utilizarea frauduloasă online a cardurilor de credit); **Crime „în" computere**, în care conținutul criminal este infracțiunea (de exemplu, abuz online și / sau materiale de exploatare sexuală a copiilor, amenințări de violență și terorism).
Jahankhani et al., 2014	**Computerul ca țintă**: de exemplu, furtul de bunuri, accesul ilicit la informații (de exemplu, lista clienților) și utilizarea acestuia pentru a obține alte beneficii, inclusiv financiare, prin amenințare; **Computerul ca instrument al infracțiunii**: de exemplu, utilizarea frauduloasă a informațiilor despre carduri și conturi bancare, conturi de conversie sau transfer, fraudă pe cardul de credit; **Computerul este incidental altor infracțiuni**: de exemplu, spălare de bani și tranzacții bancare ilegale; **Infracțiuni asociate cu prevalența computerelor**: piraterie software, încălcare a drepturilor de autor asupra programelor de computer, contrafacere a echipamentelor / programelor și furt de echipamente tehnologice.
Yar, 2006 *cit in* Jahankhani et al., 2014	**Infracțiune informatică**: trecerea frontierelor informatice ale sistemelor informatice, provocând daune drepturilor de proprietate sau proprietății (de exemplu, hacking); **Înșelăciuni și furturi informatice**: utilizarea frauduloasă a cardurilor de credit și a numerarului (informatic) prin atacarea contului bancar online și a e-bankingului; **Pornografie informatică**; **Violența informatică**, care include cyberstalking-ul și discursul de ură online; **Infracțiuni împotriva statului**, cuprinzând activități online care încalcă legile care protejează integritatea statului, cum ar fi terorismul, spionajul și divulgarea secretelor oficiale.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

În ciuda acestor clasificări și a altor categorii, nu există o conceptualizare universală a diferitelor tipuri de criminalitate informatică. Din tipologiile anterioare, se poate deduce aproximativ că criminalitatea informatică poate fi organizată în:

- Criminalitatea informatică împotriva computerelor și sistemelor informatice;
- Criminalitatea informatică activată sau practicată prin intermediul computerelor și sistemelor informatice.

Se poate concluziona, de asemenea, că, în tratarea criminalității informatice, ne referim, de fapt, la **un set de infracțiuni diverse** care implică sisteme informatice și computere ca instrumente fie pentru comiterea infracțiunilor, fie ca ținte.

1.3. Diferitele tipuri de criminalitate informatică: tendințe actuale

În următoarele secțiuni ale acestui manual, prezentăm o scurtă trecere în revistă a principalelor fenomene considerate în prezent (sau, cel puțin, a fenomenelor care merită o proeminență sau îngrijorare mai mare) în zona criminalității informatice. Trebuie menționat, totuși, că criminalitatea informatică și diferitele forme ale acesteia, inclusiv contextele în care apar, instrumentele pe care le folosesc și / sau obiectivele lor, se schimbă constant și este posibil să se includă și alte tipuri de criminalitate informatică care nu sunt acoperite de prezenta secțiune a Manualului.

De asemenea, este important să rețineți că, în ciuda cunoștințelor tot mai sporite despre diferitele fenomene ale criminalității informatice, informațiile despre scara reală a victimizării de către diferite tipuri de criminalitate informatică sunt încă incipiente și, prin urmare, ratele reale de prevalență în populație sunt necunoscute (Reep-van den Bergh & Junger, 2018). Ori de câte ori este posibil, următoarele secțiuni acoperă date din statistici oficiale privind criminalitatea informatică, anchete de victimizare criminală și / sau alte studii care permit cumva măsurarea dimensiunii diferitelor tipuri de criminalitate informatică, în special la nivel european.

IMPORTANT | STATISTICA ÎN FOCUS:

Studiul realizat de Reep-van den Bergh și Junger (2018) a căutat, prin analiza diferitelor sondaje de victimizare, să găsească o estimare aproximativă a prevalenței criminalității informatice în Europa.

Unele dintre principalele rezultate sunt rezumate mai jos:

- Între 0,6% și 3,5% din populație a raportat că a fost victimă a **fraudelor de cumpărături online** și, printre situațiile de victimizare informatică identificate, aproximativ 90% s-au referit la achiziționarea de bunuri sau servicii, plătite, dar neprimite.
- Ratele de prevalență ale **fraudelor și plăților bancare online** variază de la 0,4% la 2,2%.
- Aproximativ 3% din populație a raportat că a experimentat o formă de **agresiune informatică**, inclusiv un comportament amenințător, cu o proporție cuprinsă între 0,6% și 1,0% și *stalking* în proporții similare (0,7% până la 1,1%).
- În ceea ce privește criminalitatea informatică, în ciuda intervalelor, *hacking*-ul și *malware*-ul au fost identificate ca forme de victimizare informatică cu o prevalență mai mare: între 1,2% și 5,8% din populație au raportat că au fost victime ale hacking-ului și între 2% și 15% au raportat fiind vizat de malware.

Studiul este disponibil la: Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. Crime science, 7: 1-15.

Tipurile de criminalitate informatică menționate mai sus, precum și altele, vor fi abordate mai jos.

Cu toate acestea, este de asemenea important să contextualizați fragilitățile asociate cu măsurarea criminalității informatice: lipsa generală de cunoștințe a populației generale despre diferitele forme de criminalitate informatică, care poate duce la o subestimare a criminalității informatice experimentate și raportate în mod eficient autorităților, precum și devalorizarea dintre unele dintre fenomenele de criminalitate informatică se numără printre diferite aspecte care compromit cunoașterea dimensiunii reale a criminalității informatice (Maimon & Louderback, 2019).

1.3.1. Hacking și Cracking

Hacking-ul sau **cracking**-ul este de obicei definit **ca acces neautorizat la sistemele informatice cu intenție criminală** (Grabosky, 2016 cit în Maimon & Louderback, 2019). Acestea sunt asociate cu încălcarea informatică, care implică trecerea neautorizată a granițelor invizibile ale mediilor online (Wall, 2001 cit în Maimon & Louderback, 2019).

Hackingul include o serie de comportamente, cum ar fi **reproiectarea sistemelor hardware sau software** pentru a-și schimba funcția intenționată, precum și participarea la subcultura hackerilor (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 cit în Maimon & Louderback, 2019). Această activitate are mai multe etape, care pot include: identificarea și recunoașterea sistemelor hardware sau software vulnerabile; infiltrarea țintelor vulnerabile; modificări și reproiectare a sistemelor țintă, inclusiv instalarea de viruși și programe malware care permit accesul privilegiat la informații și date (cum ar fi date cu caracter personal, parole / acreditări de acces și informații financiare / conturi bancare) sau chiar controlul asupra sistemului în sine; acoperirea intruziunii și a modificărilor sistemului (Hughes & Delone, 2007, Wolfe și colab., 2008, Holz și colab., 2009, Waldrop, 2016, Luo și Liao, 2009 cit în Maimon și Louderback, 2019; Jahankhani și colab. ., 2014).

La fel ca majoritatea **infracțiunilor informatice**, hackingul **mediază și practicarea altor infracțiuni informatice**, servind ca mijloc pentru ca alte acte ilicite să fie posibile și să aibă succes, cum ar fi piratarea unui cont de e-mail în situații de *cyberstalking* (Leukfeldt și colab., 2006 cit în Leukfeldt și colab., 2020) și un DDoS (atac de negare a serviciului distribuit).

În ceea ce privește hacking-ul, sunt propuse și clasificări diferențiate ale hackerilor, conform intenției lor (Furnell, 2002 cit în Maimon & Louderback, 2019):

- **hackeri cu pălărie albă** (hackeri al căror acces neautorizat la sisteme este destinat să sporească securitatea acestor sisteme);
- **hackeri de pălărie neagră** (hackeri care accesează neautorizat sistemele cu intenție ilicită).

Există, de asemenea, o diferențiere conceptuală care ar trebui abordată: clasificarea hackerilor cu pălărie neagră este apropiată de conceptul de cracker, adică cineva care, spre deosebire de hackerul cu pălărie albă, profită de cunoștințele și accesul neautorizat la sistemele informatice pentru a utiliza informații și date la dispoziția lor în scopuri ilicite și / sau în scopul obținerii unui avantaj sau beneficiu personal.

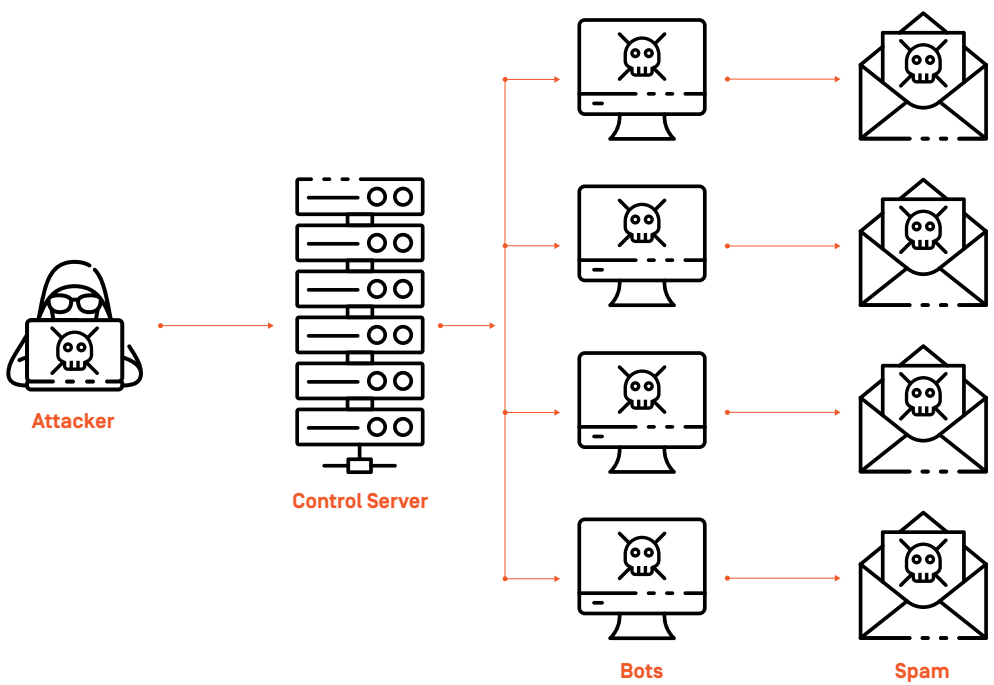
1.3.2. Spamming, Malware și DDoS [atac de negare a serviciului distribuit]

Spamming-ul sau **SPAM**-ul, acronimul pentru„Trimiterea și postarea publicității în masă", se referă la **trimiterea de date și distribuirea în masă** a e-mailurilor care fac publicitate produselor, serviciilor sau schemelor de investiții, care pot fi frauduloase și chiar conțin programe malware sau alte fișiere atașabile executabile (Rathi & Pareek, 2013).

Spamul îndeplinește trei criterii:

- Anonimat - adresa și identitatea expeditorului sunt ascunse sau lipsesc;
- Distribuirea în masă - e-mailul este trimis către un grup mare de persoane / adrese electronice;
- Nesolicitat - e-mailul nu este solicitat de către destinatari (Rathi & Pareek, 2013).

Scopul spam-ului este să înșele sau să convingă destinatarul să interacționeze cu produse, servicii sau scheme atractive. Expeditorul poate solicita numerar sau informații de securitate, cum ar fi numărul cardului de credit sau alte informații personale, înainte de a avea loc presupusul acces la produse sau servicii (Jahankhani et al, 2014).

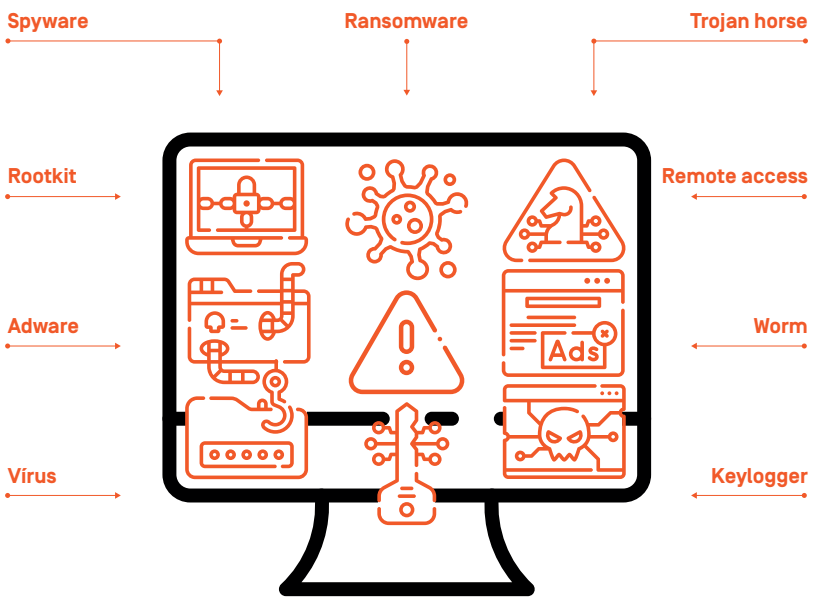


1. CRIMINALITATEA INFORMATICĂ: O ABORDARE CONCEPTUALĂ

Programele **malware** se referă la o varietate de software-uri ostile sau intruzive (de exemplu, viruși de computer, viermi[10], ransomware[11], spyware[12], adware[13], scareware[14] etc.).

Acesta este **un software destinat infiltrării ilicite a echipamentelor** pentru a provoca daune, modificări sau furt de informații. Programele malware pot lua, de asemenea, forma codului executabil, a scripturilor, a conținutului activ și a altor programe software (Aycock, 2006 cit în Reep-van den Bergh & Junger, 2018).

O schemă frecvent utilizată este publicarea de conținut cu titluri care trezesc curiozitate sau necesită un fel de acțiune „urgentă", precum și invitații la instalarea de jocuri sau sugestii pentru a vizita profiluri noi.



Atacul de negare a serviciului distribuit (DDoS), la rândul său, se referă la o încercare intenționată de a supraîncărca un anumit sistem informatic (cum ar fi cel al structurilor guvernamentale sau al companiilor mari, de exemplu), cu scopul de a-l face inutilizabil (Overvest & Straathof, 2015).

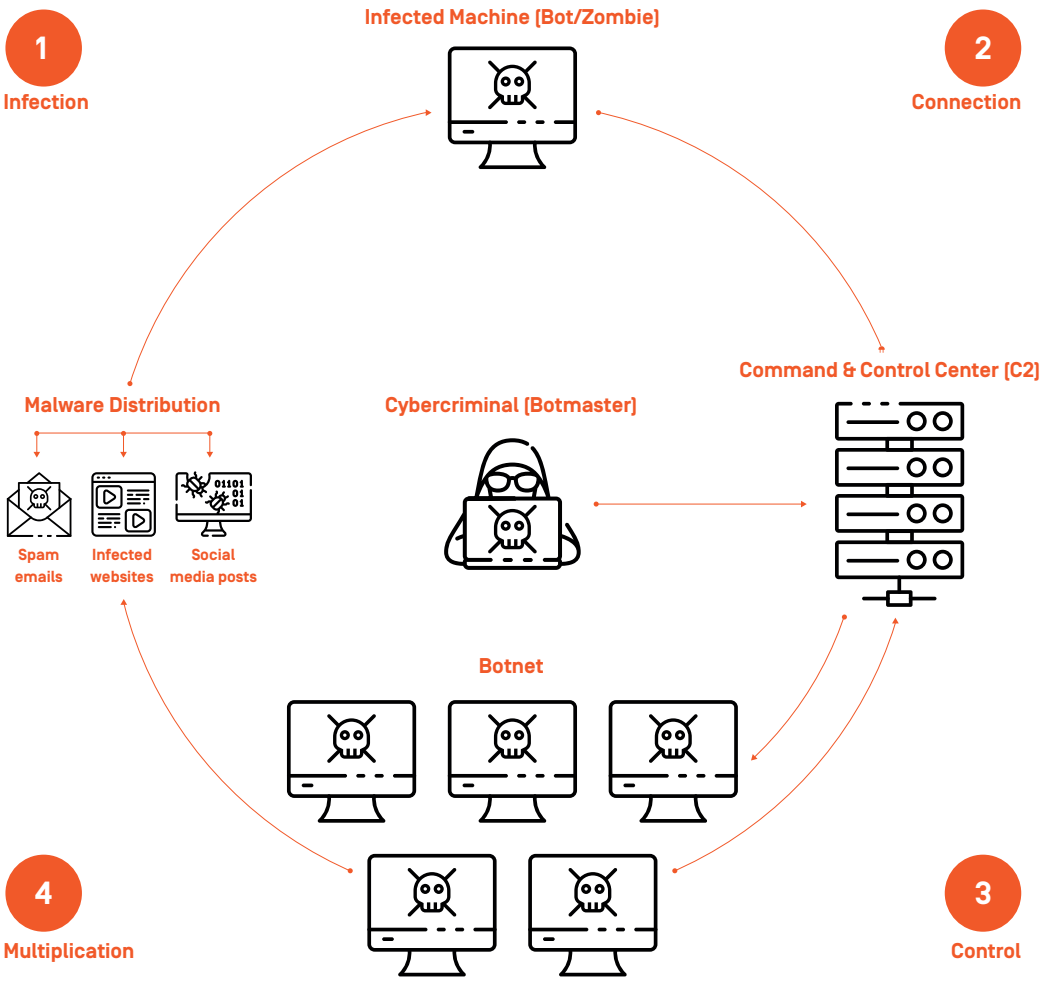
[10] Viermii sunt coduri rău intenționate care se răspândesc printr-o rețea, cu sau fără asistență umană (Kienzle & Elder, 2003).

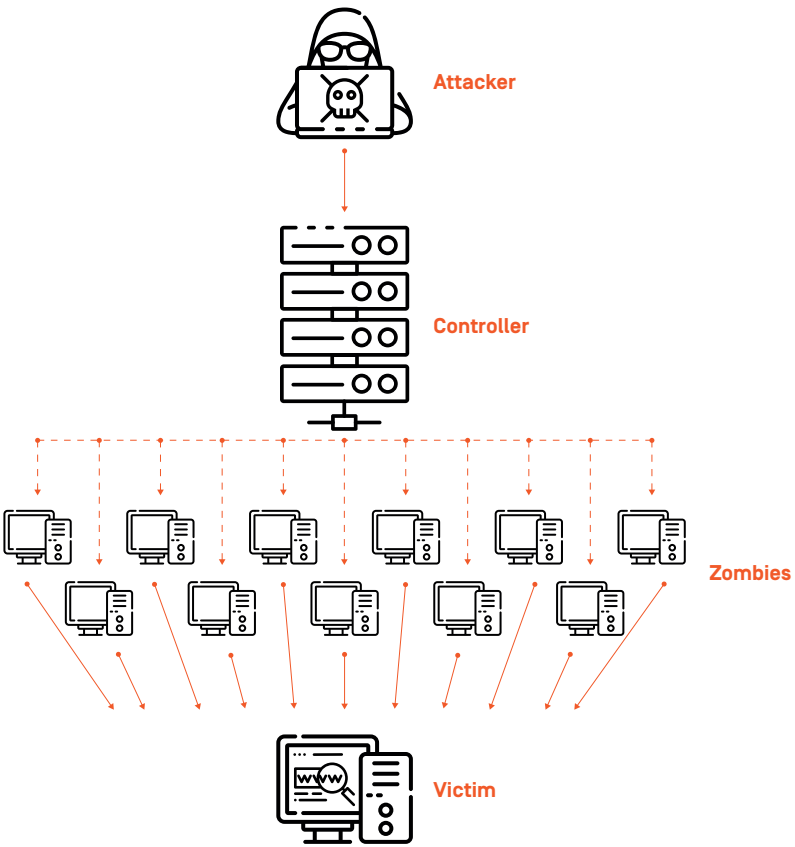
[11] Ransomware este un malware introdus în sistem prin descărcare și care creează un fișier „exe" pentru a fi rulat. Scopul poate include extorsiunea victimei prin criptarea informațiilor personale (Kansagra, Kumhar & Jha, 2016).

[12] Spyware-ul este un program automat care colectează informații despre utilizator și obiceiurile sale de utilizare a internetului și transmite aceste informații către o entitate externă, fără cunoștința și consimțământul utilizatorului.

[13] Adware este un software care afișează sau descarcă automat materiale publicitare (de obicei nedorite) atunci când utilizatorul este online (Gao, Li, Kong, Bissyandé și Klein, 2019).

[14] Scareware este o formă de malware care păcălește utilizatorul să creadă că computerul este infectat atunci când, de fapt, sistemul funcționează (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).


1
Infection
Infected Machine (Bot/Zombie)
2
Connection
Command & Control Center (C2)
Malware Distribution
Spam emails
Infected websites
Social media posts
Cybercriminal (Botmaster)
Botnet
4
Multiplication
3
Control



1.3.3. Frauda online

1.3.3.1. Fraude la cumpărături online

Cumpărăturile online se caracterizează prin incapacitatea de a inspecta fizic articolele, bunurile sau produsele înainte de cumpărare și prin lipsa de contact direct între părțile implicate în procesul de cumpărare și vânzare (Moons, 2013, van Wilsem, 2013 cit în Reep-van den Bergh & Junger, 2018), crescând riscul fraudelor la cumpărăturile online.

Frauda la cumpărături online prezintă **diferite grade de complexitate**, de la scheme simple, în care

vânzătorul promite să trimită cumpărătorului un anumit articol după efectuarea unui transfer bancar, iar acesta din urmă neprimind articolul menționat (sau primind un articol diferit de cel care a fost dobândit). Frauda poate implica, de asemenea, scheme mai elaborate care implică adesea falsificarea documentelor, cum ar fi dovezile transferului bancar.

În ceea ce privește fraudele și practica lor, există și posibilitatea de a exploata vulnerabilitățile pe site-urile de cumpărături online care stochează datele bancare ale utilizatorilor (cum ar fi detaliile cardului de credit sau de debit), care sunt accesate ilegal și apoi vândute de infractorii informatici pe dark web sau utilizat pentru tranzacții bancare fără știrea victimelor (**fraude unde cardul nu este prezent**). Furtul detaliilor bancare ale utilizatorilor pentru acest tip de fraudă are loc de obicei prin phishing, fenomen explorat în următoarele secțiuni ale acestui manual.

1.3.3.2. Fraude cu licitații pe internet

Frauda prin licitație pe internet este un alt tip de fraudă care apare atunci când articolele achiziționate sunt produse false sau obținute prin mijloace ilicite sau când vânzătorul face publicitate unor articole inexistente sau le pune la dispoziție spre vânzare. În acest tip de fraudă, este obișnuit să se utilizeze servicii de transfer bancar pentru a permite tranzacția de bani fără a fi necesară dezvăluirea identității părților implicate (Jahankhani și colab., 2014).

Frauda la licitație se bazează pe anonimat și uneori și pe utilizarea datelor de identificare false atunci când se înregistrează pe platformele sau site-urile web ale licitațiilor.

Unele dintre cele mai frecvente situații includ:

- Achiziționarea / cumpărarea de bunuri care nu sunt primite de cumpărători;
- Bunuri plătite și primite care nu corespund bunurilor dorite (de exemplu, bunul primit este semnificativ diferit de descrierea / fotografia originală);
- Nedivulgarea sau divulgarea incompletă a informațiilor relevante despre articol și / sau condițiile de vânzare;
- Nicio plată primită de vânzători.

1.3.3.3. Frauda cu carduri de credit

Frauda cu cardul de credit se referă la **utilizarea cardului de credit al altei persoane pentru uz personal, fără știrea proprietarului cardului și a emitentului** (Patel & Singh, 2013). Există mai multe metode / infracțiuni informatice care pot fi utilizate pentru a obține acces la aceste carduri și la detaliile acestora, cum ar fi phishing-ul, spam-ul sau hacking-ul (Jahankhani și colab., 2014).

În cazul **fraudării cardului de credit**, ar trebui să evidențiem **frauda *skimming***, care constă în copierea benzii magnetice a unui card de plată fără știrea sau consimțământul titularului cardului, atunci când acesta utilizează cardul respectiv la un bancomat sau la un POS.

Recent, au existat alte tipuri de atacuri, în special pe bancomate, într-un proces numit **jackpotting**. Atacul către bancomate poate avea loc prin introducerea de programe malware în sistemul informatic al echipamentului / bancomatului sau prin conexiune la hardware, numită „Black-Box". Apoi infractorul dă comanda ca bancomatele să distribuie banii pe care îi au.

1.3.3.4. Escrocherii cu romantism și întâlniri online

Escrocheriile ce implică relațiile intime apar atunci când agentul caută să stabilească o **relație de încredere și intimitate**, în special prin Internet și TIC, cu o anumită țintă, ca preludiu al **beneficiului personal, și anume al beneficiului financiar și patrimonial**.

Această formă de fraudă include de obicei:

- Crearea de profiluri false pe rețelele sociale, site-uri de întâlniri sau alte platforme de chat și interacțiune socială;
- Stabilirea contactului cu ținte aparent mai vulnerabile;
- Crearea unei legături emoționale cu ținta identificată anterior;
- Dezvoltarea unei narațiuni cu intenția de a extorca activele personale / financiare de la țintă.

Acest proces de curtare și de creare a unei relații cu victima își propune să aibă acces la banii sau alte active ale acestora, conturi bancare, carduri de credit, pașapoarte, conturi de e-mail și / sau numere de identificare personale. De asemenea, poate avea ca scop constrângerea victimei în săvârșirea infracțiunilor în numele făptuitorului.

1.3.4. Furtul de identitate online

Furtul de identitate acoperă **obținerea neautorizată de date personale și / sau confidențiale** de la o anumită victimă (cum ar fi numele, numărul de identificare personală, numărul cardului de credit etc.), precum și deținerea sau transferul și utilizarea acesteia în comiterea unei infracțiuni (Centrul de resurse pentru furtul de identitate, 2014).

Include următoarele acte cumulative:

- Obținerea de informații personale și / sau confidențiale despre o altă persoană fără știrea acestora;
- Posesia sau transferul acestor date știind că vor fi utilizate în scopuri ilicite;

- Utilizarea datelor obținute anterior pentru comiterea infracțiunilor.

Aceste acte corespund **furtului de identitate online** atunci când datele personale și / sau confidențiale ale victimei sunt obținute prin Internet și / sau atunci când datele obținute, prin orice mijloace, sunt transferate prin Internet și / sau aceste date sunt utilizate pentru ca să comită o infracțiune prin Internet.

Obiectivele sale sunt de obicei obținerea de avantaje financiare, de credit și alte beneficii, de a crea dezavantaje sau pierderi victimei (Enisa, 2010, Harrell & Lagton, 2013, Tuli & Juneja, 2015 cit în Reep-van den Bergh & Junger, 2018) și chiar să comită infracțiuni în numele victimei. Victima a cărei identitate a fost utilizată, pe lângă pierderile financiare, poate fi astfel supusă unor consecințe juridice dacă este considerată responsabilă pentru acțiunile făptuitorului.

Furtul de identitate nu este în sine o infracțiune și poate cuprinde o multitudine de infracțiuni prevăzute și pedepsite în temeiul Codului penal portughez.

1.3.5. Phishing

Phishing-ul se traduce prin trimiterea în masă a e-mailurilor - spamming - de obicei cu un link către o pagină web pe care destinatarii sunt convinși să o acceseze și apelând la motive sau acțiuni urgente. De regulă, aceste e-mailuri solicită sau evidențiază importanța „actualizării", „validării" sau „confirmării" informațiilor bancare ale destinatarilor.

Aceste e-mailuri (și paginile la care se referă) sunt false și constituie o reproducere aproximativă a comunicărilor originale făcute de bănci, instituții de credit sau altele care permit plăți online.

Când accesează astfel de pagini, utilizatorul este de obicei rugat să introducă informații bancare, făcând astfel posibil ca infractorul să le capteze și să le utilizeze în mod greșit.

Astfel, phishing-ul cuprinde diferite acte ilicite (Jahankhani și colab., 2014) și diferite etape:

- Configurarea unui **site web / pagină falsă**, care imită un site web de încredere al unei organizații de încredere sau cu o bună reputație, de obicei o organizație bancară. Această pagină de internet sau website include un formular de autentificare sau înregistrare și, de asemenea, poate redirecționa către site-ul sau pagina efectivă a organizației bancare vătămate, după utilizarea formularului.
- Crearea unui e-mail fals care, la fel ca site-ul web / pagina, imită comunicările organizației de încredere sau de încredere și **solicită acțiuni urgente din partea destinatarului** (de exemplu, avertizarea că clienții trebuie să se conecteze imediat pentru a preveni blocarea sau inactivarea conturilor / datelor de acces), cu **spamming** ulterior.
- **Obținerea informațiilor personale și / sau confidențiale** de la destinatar, inclusiv detalii

bancare, prin accesul acestora la link.
- **Utilizarea necorespunzătoare** de către autorul infracțiunii a informațiilor bancare obținute în beneficiul economic și / sau pentru săvârșirea altor infracțiuni.

IMPORTANT | STATISTICA ÎN FOCUS:

Potrivit Eurobarometrului 423[15], care a analizat percepțiile cetățenilor UE cu privire la utilizarea internetului, securitatea informatică și criminalitatea informatică, 68% dintre persoanele chestionate sunt îngrijorate de **furtul de identitate online**, urmat, în ordine descrescătoare, de îngrijorarea cu privire la software-ul cu intenții rele / malware (66%) , **fraudă online**, și anume fraudă cu carduri bancare (63%) și **piratarea** conturilor lor de e-mail și de pe rețelele sociale (60%).

În plus, 47% dintre respondenți au raportat că au fost deja ținta programelor malware și 31% au declarat că au fost deja victima încercărilor de **phishing**.

1.3.6. Abuzul sexual și exploatarea copiilor prin intermediul internetului

Abuzul sexual asupra copiilor este definit de Organizația Mondială a Sănătății - OMS (2017) ca implicarea unui copil, adică a oricărei persoane cu vârsta sub 18 ani, în activitatea sexuală:

- pe care copilul nu o înțelege pe deplin;
- pentru care copilul nu poate acorda consimțământul informat sau nu este pregătit pentru dezvoltare;
- care încalcă legile actuale.

Pot fi luate în considerare diferite tipuri de abuz sexual asupra copiilor (OMS, 2017):

- **Abuz sexual fără contact**, care include amenințări de abuz sexual, hărțuire sexuală, *grooming* (*curtare*), solicitare sexuală, expunerea copilului la conținut / materiale pornografice, printre alte forme de abuz care nu implică contact direct între victimă și infractor;
- **Abuz sexual cu contact**, care include, de exemplu, practicarea sexului vaginal, anal și / sau oral cu copilul, prin penisuri, părți ale corpului sau obiecte, precum și alte acte sexuale, cum ar fi sărutarea, mângâierea și atingerea necorespunzătoare.

Utilizarea tot mai mare și mai timpurie a **internetului și a rețelelor sociale de către copii**, combinată cu supravegherea familială redusă, inexistentă și / sau ineficientă, mărește **expunerea acestora la abuzuri sexuale și exploatare prin internet** (Consiliul Europei, 2007 cit în APAV, 2019 ; Livingston & Smith, 2014).

[15] Informații suplimentare și detaliate despre acest Eurobarometru - Eurobarometru special 423: Securitate informatică - este disponibil la https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

1. CRIMINALITATEA INFORMATICĂ: O ABORDARE CONCEPTUALĂ

IMPORTANT | STATISTICA ÎN FOCUS:

Conform bazei de date a INTERPOL[16], *International Child Sexual Exploitation* (ICSE), în 2018 au fost înregistrate peste 1,5 milioane de imagini și videoclipuri și 19.400 de copii au fost identificați drept victime ale abuzurilor și exploatării sexuale la nivel mondial.

În urma unei selecții aleatorii de videoclipuri și imagini din baza de date ICSE menționată anterior, INTERPOL și ECPAT International au publicat un raport comun intitulat *Către un indicator global privind victimele neidentificate în materialul de exploatare sexuală a copiilor* în 2018 și subliniem următoarele rezultate:

- 92% dintre infractorii vizibili erau bărbați;
- 65% dintre victimele neidentificate erau fete;
- Peste 60% dintre victimele neidentificate erau pre-pubescente, inclusiv bebeluși și copii mici;
- Cu cât victima este mai tânără, cu atât abuzul este mai sever;
- 84% din imagini conțineau conținut explicit de abuz sexual asupra copiilor, inclusiv activitate sexuală explicită.

Unele forme de abuz sexual și exploatare a copiilor prin intermediul internetului sunt abordate mai jos[17].

1.3.6.1. Abuzul sexual online asupra copiilor

Abuzul sexual online, ca un concept cuprinzător, poate fi definit ca cuprinzând **orice formă de abuz sexual asupra copiilor într-un context online**, care include manifestări diferite, de la abuzuri sexuale fără contact facilitate de TIC și Internet, rețelele sociale sau alte platforme, precum ca hărțuire și îngrijire, la partajarea conținutului pe dark web (imagine și / sau audio) a abuzului și exploatării sexuale a copiilor, utilizând fotografii sau videoclipuri realizate anterior.

1.3.6.2. Exploatarea sexuală a copiilor online

Conceptul de exploatare sexuală a copilului se distinge de alte forme de abuz deoarece este caracterizat prin extracție, câștig și beneficii care rezultă din supunerea copilului la un anumit tip de act sexual. Este dificil să îl disociem în mod clar de conceptul de abuz sexual, dar, de regulă, exploatarea sexuală presupune exploatarea caracteristicii, situației sau stării unui copil, iar beneficiile sunt colectate de făptuitor, de terți sau chiar de copilul însuși (așa cum este cazul, de exemplu, al copilului supus unor situații de abuz sexual în schimbul iubirii și afecțiunii de către adulți semnificativi).

Exploatarea sexuală a copiilor online include toate actele de natură sexuală cu o conexiune TIC comise împotriva unui copil, cum ar fi:

- Exploatarea sexuală efectuată în timp ce copilul victimă folosește internetul și TIC, inclusiv

[16] Informații suplimentare și detaliate sunt disponibile la adresa https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[17] Pentru informații detaliate despre terminologie și diferite forme de abuz și exploatare sexuală a copiilor, vă rugăm să consultați EPCAT International și EPCAT Luxembourg *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, disponibile la adresa: http://luxembourgguidelines.org/english-version/.

seducerea, manipularea și amenințarea copilului de a efectua acte sexuale în fața unei camere web, de exemplu;
- Identificarea și / sau *grooming*-ul potențialelor victime online pentru exploatare sexuală (indiferent dacă exploatarea și abuzul au loc online sau offline);
- Distribuirea, divulgarea, importul, exportul, oferta, vânzarea, deținerea sau accesul online conștient la materiale de exploatare sexuală a copiilor (chiar dacă conținutul de abuz sexual conținut în material a fost efectuat offline).

1.3.6.3. Abuzul sexual online în direct asupra copiilor

Acest fenomen implică **practicarea actelor sexuale cu copiii și transmiterea lor în direct**, prin intermediul serviciilor de streaming live, făcând astfel posibilă urmărirea lor de către alte persoane. Vizionarea poate implica plata prealabilă a unei anumite sume, iar spectatorii pot avea chiar posibilitatea să dicteze sau să definească cursul actelor de abuz sexual și exploatare practicate împotriva copilului.

Transmiterea în direct înseamnă că datele sunt transmise instantaneu și cu un risc mai redus, deoarece nu necesită descărcarea niciunui fișier și, imediat ce transmisia este întreruptă, materialul dispare, ceea ce face dificilă investigarea infracțiunii, colectarea probelor și identificarea victimelor și făptașii.

Abuzul sexual asupra copiilor în direct implică diferite forme de abuz și exploatare sexuală asupra copiilor, inclusiv producerea și distribuirea materialelor de abuz și exploatare sexuală asupra copiilor și prostituția. Reprezintă **o formă dublă de victimizare sexuală a copilului**: în primul rând, copilul este forțat sau, într-un fel, este condus să participe la activități sexuale, singur sau cu alte persoane; simultan, activitatea sexuală este transmisă în direct, prin TIC și vizualizată de la distanță de alte persoane.

1.3.6.4. Grooming-ul online

Grooming-ul (curtarea) online poate fi definită ca **un proces de manipulare și o formă de solicitare** a copiilor. De obicei, începe cu o abordare non-sexuală prin Internet și TIC, inclusiv jocuri online și rețele sociale, pentru a stabili o relație de încredere cu copilul și pentru a-l convinge pe copil să se întâlnească față în față, astfel încât făptuitorul să poată consuma abuzul sexual. Stabilirea unei relații de încredere cu copilul, mediată de internet și TIC, poate avea ca scop și convingerea copilului să producă și să împărtășească conținut sexual[18].

Grooming-ul online permite infractorilor să selecteze tipul de victimă pe care doresc să o manipuleze și să o ademenească. În plus, grooming-ul online permite atragerea simultană a unui număr mare de victime, printre alte avantaje pentru făptuitor, precum anonimatul, păstrarea identității lor reale și gestionarea celorlalte „identități" cu care se prezintă țintelor selectate.

[15] În contextul conținutului sexual auto-generat, putem include, spre exemplu, sexting-ul, ca formă de auto-producție a conținutului - text, imagini și / sau videoclipuri - de natură sexuală și partajarea acestuia, de obicei într-un în mod consensual și între colegi. Cu toate acestea, poate fi produs sub presiune sau constrângere sau chiar poate duce la partajarea non-consensuală a conținutului produs.

Ca urmare a acestei forme de abuz și exploatare sexuală, infractorul poate supune copilul la amenințări și șantaj pentru a disemina sau a împărtăși conținutul sexual auto-generat, cu scopul de a atrage favoruri sexuale, bani sau alte beneficii. Acest fenomen se numește **extorcare sexuală a copilului**.

IMPORTANT | PRACTICI IN FOCUS:

Childline[19] este un serviciu gratuit și confidențial pus la dispoziția copiilor și tinerilor din Marea Britanie, care abordează o gamă largă de probleme și probleme care pot afecta aceste grupe de vârstă.

Printre mai multe subiecte, serviciul conține informații despre comportamentul sigur în utilizarea internetului și a TIC, precum și un mecanism online pentru raportarea partajării / diseminării conținutului sexual auto-produs.

Mecanismul de raportare este disponibil la:https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/.

1.3.6.5. Material online de abuz sexual și exploatare a copiilor

IMPORTANT | STATISTICI ÎN FOCUS:

Conform Eurobarometrului 423 deja menționat, 7% dintre persoanele chestionate au raportat că au fost expuse accidental la **abuzuri și materiale de exploatare online ale copiilor**.

Expresiile **material de abuz sexual asupra copiilor și material de exploatare sexuală a copiilor** caută să înlocuiască, cel puțin în contexte non-legale, conceptul de pornografie infantilă (terminologie care figurează încă în legislația națională și internațională) și acoperă:

- No caso do material de abuso sexual de crianças, a conteúdo e material que representa ou retrata atos de abuso sexual de crianças e/ou os órgãos sexuais de crianças;
- No caso de material de exploração sexual de crianças, enquanto terminologia mais abrangente, que respeita a todo o material que retrate ou represente crianças de forma sexualizada.

Această modificare a terminologiei se bazează pe argumentul că orice material care reprezintă un copil într-un mod sexualizat este de fapt o formă de abuz sexual al copilului și exploatare sexuală a copilului și nu ar trebui descris ca „pornografie".

Materialul de abuz și exploatare sexuală a copiilor generat digital sau computerizat, în totalitate sau parțial, este considerat și material de exploatare și abuz sexual al copiilor.

[19] Informații suplimentare detaliate sunt disponibile la adresa: https://www.childline.org.uk/.

1.3.7. Cyberbullying, cyberstalking și alte forme de agresiune online în relațiile interumane

Bullying-ul este un fenomen de violență între colegi/semeni care implică sau implică săvârșirea unui comportament agresiv și violent de către un agresor sau un grup de agresori împotriva unei victime sau a unui grup de victime cu scopul de a le răni, de a le provoca rău sau suferință (APAV, 2011).

Cyberbullying-ul implică utilizarea TIC și a internetului, cu scopul de a ataca verbal victima și / sau de a contribui la excluderea și izolarea socială a acesteia. Unele dintre comportamentele care sunt incluse în această formă de agresiune online sunt: diseminarea informațiilor negative / false cu intenția de a defăima victima (prin apeluri telefonice, mesaje text, mesaje video, e-mail, cameră de chat, site-uri web, rețele sociale); hărțuirea victimei (folosind aceleași mijloace) (APAV, 2011; Jahankhani și colab., 2014).

Cyberbullying-ul se distinge de forme mai convenționale de intimidare prin posibilitatea de a fi făcut în orice moment al zilei, indiferent de necesitatea unui contact direct între victimă și agresor; potențialul de anonimat al agresorului; potențialul ridicat de „publicitate" și audiențe (poate fi partajat infinit pe rețelele sociale sau pe orice altă platformă de comunicare pe internet unde a fost inițiată / publicată și chiar între platforme); și dificultatea de a elimina conținutul creat (Stopbullying. Gov, 2017).

IMPORTANT | STATISTICI ÎN FOCUS:

Conform rezultatelor sondajului UE KIDS ONLINE[20], care a implicat 19 țări din Uniunea Europeană, cu privire la utilizarea internetului și practicile și experiențele online ale copiilor cu vârste cuprinse între 9 și 16 ani, în medie 5% dintre copii au raportat că au **fost hărțuiți informatic** în ultimele 12 luni înainte de sondaj.

În același sondaj, aproximativ 22% dintre copiii participanți au raportat că au primit deja **mesaje cu conținut sexual**. A se vedea secțiunile anterioare, în care sunt abordate diferite forme de abuz și exploatare sexuală a copiilor prin intermediul internetului.

Conform celor mai recente date din studiul transnațional *Health Behavior in School-Aged Children*[21], efectuat în mod regulat de Organizația Mondială a Sănătății (OMS), prevalența **hărțuirii informatice** este mai mare decât cea identificată în sondajul anterior: respectiv, 12% și 14% din adolescenții băieți și fete au raportat că au experimentat agresiune informatică.

În ceea ce privește diferitele forme de intimidare informatică, putem evidenția următoarele comportamente de agresiune online cu caracter sexual:

- Împărtășirea online a zvonurilor sau minciunilor cu privire la comportamentul sexual al victimei;
- Utilizarea online a unui limbaj sexual ofensator sau discriminatoriu îndreptat împotriva victimei;

[20] | Informații suplimentare detaliate despre studiu sunt disponibile la 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.

[21] Informații suplimentare detaliate sunt disponibile în raportul studiului: 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.

- Furt de identitate care vizează partajarea conținutului sexual și / sau hărțuirii sexuale împotriva celorlalți care utilizează identitatea victimei;
- Schimbul online de informații cu privire la intimitatea victimei, într-un mod non-consensual, ca strategie de perpetuare a comportamentelor de agresiune și hărțuire pe scară largă.

De asemenea, am putea adăuga *body shaming* prin Internet și TIC, ceea ce implică schimbul de comentarii disprețuitoare despre aspectul fizic al victimei și ieșirea, atunci când cineva dezvăluie (sau amenință să dezvăluie) public, prin Internet și TIC, informații despre orientarea sexuală a victimei sau identitatea de gen fără știrea și permisiunea lor.

Cyberstalking-ul poate fi definit ca o formă de stalking care, deși este intruzivă, repetitivă și persistentă și provoacă frică victimei (caracteristici ale acestei forme de persecuție și hărțuire persistentă), se practică folosind internetul și TIC cu scopul de a amenința și hărțui victima (Maran & Begotti, 2019).

Practicile de cyberstalking pot include diferite comportamente prădătoare: efectuarea mai multor încercări nedorite de a contacta victima, prin telefon, e-mail și rețele sociale; instalarea de spyware pe computerul victimei; accesarea conturilor de e-mail și / sau rețele sociale ale victimei fără autorizația victimei, pentru a monitoriza informațiile private și viața de zi cu zi a victimei și / sau pentru a acționa folosind identitatea acestora (Martellozzo & Jane, 2017).

Cyberstalking-ul poate preceda practicarea altor forme de stalking în contexte convenționale sau chiar poate avea loc ca parte a unei campanii de stalking și hărțuire care are loc atât online, cât și offline. Delincvenții pot fi persoane pe care victima le cunoaște, inclusiv prieteni și colegi de muncă, precum și foști parteneri sau persoane necunoscute (Maran și Begotti, 2019).

IMPORTANT | STATISTICI ÎN FOCUS:

Potrivit unui sondaj european privind violența împotriva femeilor, peste 40.000 de femei chestionate în diferite state membre ale Uniunii Europene, 5% au raportat că au fost victime ale unei forme de **cyberstalking** de la vârsta de 15 ani.

Statele membre care s-au remarcat au fost Suedia, cu cea mai mare prevalență, la 14%, și Spania, cu cea mai mică prevalență, la 2%.

În ceea ce privește violența online în relațiile interpersonale, putem evidenția, pe lângă hărțuirea informatică și cyberstalking-ul, divulgarea non-consensuală a imaginilor și videoclipurilor - aceasta se referă la schimbul de imagini intime, inclusiv fotografii, filme și / sau înregistrări video, fără acordul persoanei care are nuditatea, părțile corpului, inclusiv organele sexuale și / sau activitatea sexuală expuse.

Motivațiile pentru divulgarea acestui conținut pot include:

- **Extorcarea sau constrângerea sexuală a victimei**, în care făptuitorul, după ce a primit de la victimă, de obicei în mod consensual, videoclipuri și / sau fotografii de natură sexuală, amenință diseminarea lor dacă victima nu oferă conținut nou generat de sine de natură sexuală sau nu este de acord cu întâlnirea față în față cu agresorul.

- **Răzbunarea**, denumită adesea *revenge porn*, implică divulgarea non-consensuală a imaginilor intime - fotografii, filme și / sau înregistrări video ale unui partener, de obicei după încheierea relației, ca formă de represalii. Acesta este un fenomen obișnuit în domeniul violenței în relațiile intime în care, după destrămarea relației, sunt difuzate imagini sexuale și / sau videoclipuri ale fostului partener (sau există inflexiuni pentru a le disemina), către familie și prieteni, prin intermediul rețelelor sociale sau chiar pe site-uri pornografice.

IMPORTANT | PRACTICA ÎN FOCUS:

Facebook oferă, în *Nu Fără Consimțământul Meu*, o gamă de resurse de informații asociate cu extorcarea sexuală și diseminarea neconformă a imaginilor și videoclipurilor.

Nu fără consimțământul meu are, de asemenea, un spațiu pentru raportarea partajării / difuzării non-consensuale a imaginilor și videoclipurilor, precum și un ghid cu instrucțiuni pentru eliminarea conținutului online.

Informații suplimentare detaliate sunt disponibile la: https://www.facebook.com/safety/notwithoutmyconsent.

1.3.8. Alte forme de infracțiuni informatice

Terorismul informatic este o formă de terorism care folosește informații, computere, rețele și infrastructură tehnică pentru a desfășura activități teroriste. Datorită importanței acestor componente de rețea de interconectare, terorismul informatic ar putea fi considerat potențial mai dăunător decât terorismul tradițional. În special, terorismul informatic vizează infrastructura financiară și de afaceri, precum și infrastructura guvernamentală, controlul traficului aerian și dosarele medicale, cu avantajul că poate fi realizat cu resurse financiare modeste, anonimat și de la distanță (Hansen, Lowry, Meservy & McDonald, 2007).

Intenția terorismului informatic este de a **incapacita și / sau reduce drastic disponibilitatea resurselor de calcul ale unei organizații, entități sau infrastructuri**: pentru o companie privată, acest tip de atac poate duce la pierderi financiare; pentru o entitate guvernamentală, aceasta poate duce la incapacitatea de a-și îndeplini misiunea (Kratchman, Smith & Smith, 2008).

Conceptul de terorism informatic este asociat cu distrugerea și / sau incapacitarea **infrastructurilor**

critice, care, dacă sunt compromise, pot avea un impact debilitant asupra securității naționale, economiei și situației sociale a unei țări date (Dunn & Wigert, 2004 cit în Yar & Steinmetz, 2019). În cadrul acestor infrastructuri critice, am putea include rețele de comunicații, energie, apă, alimente, servicii de urgență și servicii de sănătate, precum și simboluri ale coeziunii naționale (Milone, 2003 cit in idem). Dintre aceste infrastructuri, cele din sectoarele informației și telecomunicațiilor se remarcă prin rolul lor central în funcționarea celorlalte infrastructuri critice ale unei țări (Dunn & Wigert, 2004 cit in idem).

Pentru practicarea terorismului informatic, pot fi comise mai multe dintre infracțiunile dependente informatic menționate în acest manual.

Pe de o altă parte, am putea include **discursuri de ură online**, care include toate formele de comunicare și exprimare, prin Internet și TIC, care promovează, difuzează, incită sau caută să justifice ura rasială, xenofobia, antisemitismul și alte forme de ură bazate pe ură asupra intoleranței împotriva unei persoane sau a unui grup de persoane.

IMPORTANT | STATISTICI IN FOCUS:

În *Flash Eurobarometer 469 - iunie 2018*[22], respondenții au fost întrebați despre tipul de conținut ilegal întâlnit accidental online. Printre mai multe opțiuni, **discursul de ură** a fost cel mai menționat tip de conținut ilegal în 10 țări, în special în Malta (55%), Republica Cehă (53%), Bulgaria (52%) și Polonia (50%).

Respondenții care au raportat că au vizionat cel puțin un tip de conținut ilegal online au fost întrebați despre acțiunile lor:

- A maioria (59%) afirmou não ter efetuado qualquer ação após a visualização do referido conteúdo ilegal.
- De entre as ações realizadas, a mais comum foi informar o prestador de serviços de Internet (21%).
- Cerca de uma em cada dez pessoas inquiridas contactou diretamente a pessoa ou entidade responsável pelo conteúdo (9%) ou alertou a polícia/autoridades (8%).

Utilizarea crescândă a internetului, a TIC și a rețelelor sociale a fost însoțită de proliferarea **discursurilor de ură online împotriva anumitor grupuri de oameni** (Banks, 2010 cit în Martellozzo & Jane, 2017). Această proliferare se bazează pe un set de caracteristici asociate Internetului și TIC, dintre care putem evidenția (Yar & Steinmetz, 2019):

- Este un instrument eficient și ieftin, bazat pe o investiție financiară redusă, cu capacitatea de a disemina discursurile de ură către publicul larg;
- Prezintă un risc mai mic de detectare și identificare, permițând anonimatul și păstrarea identității;
- Permite accesul la canalele de comunicare care nu ar fi disponibile altfel pentru diseminarea acestui tip de discurs;

[22] Informații suplimentare detaliate sunt disponibile la https://ec.europa.eu/digital-single-market/en/news/flash-eurobarometer-illegal-content .

- Permite conținutul și formatul transmiterii informațiilor să fie adaptate în funcție de public și de grupurile țintă.

IMPORTANT | PRACTICI IN FOCUS:

În mai 2016, Comisia Europeană și patru platforme digitale (Facebook, Youtube, Twitter și Microsoft) au anunțat un **Cod de conduită împotriva discursului de ură online**[23], la care au aderat alte companii.

Unul dintre obiectivele acestui cod este eliminarea mai rapidă a conținutului online de ură, respectiv în termen de 24 de ore, cu scopul de a reduce numărul de persoane la care ajunge.

1.4. Figurile întunecate ale criminalității informatice

Cifrele legate de criminalitate informatică pe care le-am rezumat în secțiunile anterioare ale acestui manual nu prezintă, în ciuda expresivității și dimensiunii lor semnificative, realitatea efectivă a criminalității informatice.

Prevalența precisă a criminalității informatice este necunoscută. Este probabil să fie **un număr mai mare de infracțiuni informatice nedetectabile, nedeclarate, neinvestigate și nerezolvate**, având în vedere invizibilitatea și complexitatea dovezilor digitale asociate cu apariția acesteia, eventualele lacune legislative și chiar natura transnațională a criminalității informatice (Koops, 2010; Cangemi , 2004 cit în Yucedal, 2010).

În plus, reticența pe scară largă a victimelor criminalității informatice de a raporta (Koops, 2010), fie din frică, ignoranță și / sau devalorizare a faptelor la care au fost supuse, contribuie, de asemenea, semnificativ la lipsa de cunoștințe despre amploarea reală a criminalității informatice.

Există mai multe explicații pentru nedeclararea situațiilor de criminalitate informatică și, în consecință, pentru decalajul dintre numărul criminalității informatice care intră în atenția autorităților competente și criminalitatea informatică „reală" (Goucher, 2010; Kanayamaa, 2017; Maimon & Louderback , 2019; Leukfeldt și colab., 2020) și subliniem::

- Lipsa de cunoaștere sau recunoaștere a victimelor infracțiunilor informatice asupra faptelor la care au fost supuse drept forme de infracțiune;
- Sentimente de rușine, de vinovăție și de învinovățire pentru victimizarea informatică;
- Devalorizarea daunelor și pierderilor cauzate de criminalitatea informatică;
- Reticența sau rezistența victimelor de a raporta criminalitatea informatică autorităților competente;
- Eșecul identificării beneficiilor asociate cu raportarea criminalității informatice către autoritățile

competente, având în vedere eșecul potențial al investigațiilor privind criminalitatea informatică și daunele aparent limitate cauzate de criminalitatea informatică (cel puțin în ceea ce privește daunele și impacturile resimțite / percepute de fiecare victimă individuală);
- Lipsa de familiaritate și cunoștințe a forțelor de securitate cu privire la criminalitatea informatică;
- Lipsa instruirii specifice criminalității informatice pentru forțele de securitate și lipsa resurselor financiare pentru cercetări ulterioare;
- Absența unor servicii sau răspunsuri de sprijin specifice sau specializate, diferențiate de răspunsurile tradiționale la victimele infracțiunilor „convenționale", care ar putea ajuta victima criminalității informatice în obținerea ajutorului / conectarea la resursele disponibile;
- Lipsa sistemelor și mecanismelor accesibile (în special prin intermediul internetului) și raportarea simplă a criminalității informatice.

Recunoscând dificultățile existente, subliniem în acest manual exemple de răspunsuri, servicii și mecanisme existente, care raportează eforturile depuse pentru a promova și facilita accesul la servicii de asistență, informații, precum și mecanisme online pentru raportarea situațiilor de criminalitate informatică.

IMPORTANT | PRACTICI ÎN FOCUS:

EUROPOL - *Agenția Uniunii Europene pentru Cooperare în Aplicarea Legii* oferă pe site-ul său web o pagină în care este posibilă accesarea mecanismelor de raportare a criminalității informatice (inclusiv raportarea online, acolo unde este cazul) existente în diferite state membre.

Această pagină este disponibilă la: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online .

IMPORTANT | PRACTICI ÎN FOCUS:

Action Fraud este centrul național de plângeri din Marea Britanie pentru escrocherii online și alte infracțiuni informatice.

În plus față de asistența telefonică oferită, Action Fraud oferă un instrument de raportare online, accesibil la: https://reporting.actionfraud.police.uk/login .

În cazul **abuzului sexual și al exploatării copiilor prin internet**, alte obstacole sunt asociate cu dezvăluirea experienței de victimizare a copilului, cum ar fi:

- Sentimente de vinovăție și rușine pentru victimizarea informatică pe care au experimentat-o;
- Un sentiment de (auto) responsabilitate datorat percepției victimei că este într-un fel sau altul

complice sau părtașe la situația de victimizare informatică;
- Teama de represalii de către autorul criminalității informatice și / sau pedeapsa de către cei responsabili legal în caz de divulgare;
- Teama de a fi discreditat;
- Teama de a pierde recompensele pe care le-ar putea primi de la autorul actelor de abuz sexual și exploatare în schimbul practicării, participării și / sau producției de conținut sexual;
- Eșecul identificării situațiilor de abuz și exploatare sexuală ca acte ilegale și / sau interpretării acestora ca manifestări de afecțiune.

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

IMPORTANT | PRACTICI ÎN FOCUS:

INHOPE[24] este o rețea formată în prezent din 46 de *linii de asistență telefonică* din diferite țări, inclusiv din statele membre ale Uniunii Europene, care vizează combaterea abuzului sexual online și a materialului de exploatare a copiilor.

Asociația Portugheză pentru Sprijinirea Victimelor (APAV) este responsabilă, în **Portugalia**, de funcționarea Liniei de Internet sigur [Linha Internet Segura], în cadrul consorțiului Centrul de Internet Sigur [Centro Internet Segura], promovat de Fundația pentru Știință și Tehnologie. Pe lângă furnizarea de asistență și informații cu privire la problemele de siguranță pe Internet, intervenția Linha Internet Segura include o platformă care permite și facilitează **raportarea anonimă a conținutului ilegal pe internet**, cu accent pe materialele abuzive și de exploatare sexuală a copiilor online și incitarea și promovarea rasismului , xenofobiei și alte forme de violență.

Platforma de raportare este disponibilă la: https://www.internetsegura.pt/.

În **Germania**, Safer Internet Center[25] este, de asemenea, o platformă care oferă informații de siguranță cu privire la utilizarea internetului familiilor, copiilor și tinerilor și profesorilor. Include, de asemenea, linii telefonice de asistență și o platformă pentru raportarea materialelor de abuz și exploatare sexuală a copiilor online: https://www.jugendschutz.net/hotline/.

În **România**, una dintre țările care fac parte, de asemenea, din INHOPE, Salvați Copiii România are disponibil un mecanism / formular electronic care facilitează raportarea conținutului ilegal online. Consultați https://oradenet.salvaticopiii.ro/esc-abuz

În ceea ce privește **criminalitatea informatică împotriva entităților colective**, și anume organizațiile și companiile, mici sau mari, studiile indică o prevalență ridicată a criminalității informatice, în special a **infracțiunilor dependente de informatică** (Rantala, 2008 cit în Maimon & Louderback, 2019; Saini, Rao și Panda, 2012). Paradoxal, ratele de raportare identificate sunt destul de scăzute, ceea ce poate fi asociat, printre alte motive, cu:

[25] Informații suplimentare și detaliate sunt disponibile la adresa https://www.inhope.org/EN .

- Teama de a compromite reputația entității, imaginea sa publică și / sau marca, produsele și / sau serviciile pe care le oferă;
- Teama de a pierde încrederea societății și a cetățenilor în activitatea entității și în calitatea și fiabilitatea acesteia;
- Minimizarea posibilelor pierderi financiare asociate cu impacturi potențiale asupra dimensiunilor indicate mai sus;
- Faptul că infracțiunile informatice au fost practicate de către cineva din interiorul entității.

2. CADRUL LEGAL AL INFRACȚIUNILOR INFORMATICE

2.1. Criminalitatea informatică, așa cum este văzută de Consiliul Europei

Având în vedere necesitatea de a proteja drepturile fundamentale în spațiul informatic și de a proteja împotriva consecințelor socio-economice grele asociate cu practicarea criminalității informatice, reglementarea penală a conduitei ilegale care are, în esența sa, sau ca element facilitator, utilizarea mijloacelor informatice este crucial. În acest sens, condamnarea expresă a acestor conduite și actualizarea lor constantă poartă în sine nu numai un mesaj de descurajare pentru eventualii agenți ai infracțiunilor, ci și faptul că lupta împotriva criminalității informatice se află tot mai mult în fruntea agendelor politice ale statelor[26].

Cel mai relevant instrument internațional în domeniul criminalității informatice este Convenția Consiliului Europei privind criminalitatea informatică din 23 noiembrie 2001, care vizează „protecția societății împotriva criminalității informatice, *inter alia*, prin adoptarea legislației corespunzătoare și încurajarea cooperării internaționale", în scopul „derulării investigațiilor penale și procedurilor privind infracțiunile legate de sistemele și datele informatice mai eficiente și permiterea colectării probelor în formă electronică"[27]. În acest scop, Convenția solicită statelor semnatare să își adapteze legislația penal primară și secundară la caracteristicile specifice ale acestor infracțiuni, cu scopul armonizării legislației, inclusiv a instrumentelor procedurale și de colectare a probelor adecvate, și simplificarea cooperării internaționale pentru a facilita și a accelera detectarea, investigația, strângerea probelor și urmărirea penală. În cele din urmă, urmărește, de asemenea, armonizarea dreptului penal primar și, pentru a spori urmărirea penală și ancheta de către poliție și autoritățile judiciare, Convenția sugerează, de asemenea, punerea în aplicare a măsurilor procedurale specifice adecvate acestui tip de infracțiuni și promovează cooperarea internațională.

În ceea ce privește protecția împotriva abuzului sexual și a exploatării minorilor, documentul principal este Convenția privind protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale, cunoscută în mod obișnuit drept Convenția de la Lanzarote[28]. În vigoare de la 1 iulie 2010, a extins infracțiunile pentru a acoperi toate tipurile posibile de infracțiuni sexuale împotriva copiilor. O relevanță deosebită în criminalitatea informatică este caracterizarea comportamentelor de grooming a copiilor prin expunerea la conținut sexual și ilegal legat de exploatarea sexuală și abuzul minorilor. Convenția acoperă, de asemenea, abuzurile sexuale în cadrul familiei sau „cercul de încredere" al copilului, precum și actele desfășurate în scopuri comerciale sau de profit. În consecință, statele sunt îndemnate să elaboreze legislație specifică care să criminalizeze orice conduită menționată în Convenție, să investigheze și să trimită în judecată autorii infracțiunilor și să promoveze măsuri preventive care să țină cont de interesul superior al copilului. În final, este promovată și cooperarea internațională între state[29].

2.2. Criminalitatea informatică în dreptul Uniunii Europene

În cadrul Uniunii Europene (UE), au fost adoptate mai multe instrumente privind criminalitatea informatică. În 2013, printr-o comunicare comună către Parlamentul European, Consiliul, Comitetul

[26] Comunicare comună către Parlamentul European și Consiliu: Reziliență, descurajare și apărare: construirea unei securități cibernetice puternice pentru UE; JOIN(2017) 450 final; Brussels, 13.9.2017; pp. 2-3.

[27] Convenția Consiliului Europei privind criminalitatea informatică, Budapest, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

[28] Convenția Consiliului Europei privind protecția copiilor împotriva exploatării și abuzurilor sexuale, https://rm.coe.int/protection-of-children-against-sexual-exploitation-and-sexual-abuse/1680794e97.

[29] Pentru mai multe informații, consultați https://rm.coe.int/information-note-the-council-of-europe-convention-on-the-protection-of/16807962a7.

Economic și Social European și Comitetul Regiunilor au definit Strategia de securitate informatică a Uniunii Europene[30]. Aceasta definește drept piloni cheie ai strategiei armonizarea politicilor și stabilirea mecanismelor de cooperare între statele membre pentru a asigura securitatea informatică și respectarea principiilor democratice ale UE. În acest scop, propune crearea unei legislații adecvate privind securitatea informatică, menită să dezvolte resursele industriale și tehnologice pentru a asigura securitatea digitală și crearea de unități naționale de combatere a criminalității informatice. Astfel, comunicarea prevede sinergii cu sectorul privat pentru crearea rezilienței digitale. Pe de altă parte, prevede, de asemenea, măsuri preventive, cum ar fi campanii de conștientizare și formare specializată asupra fenomenului. Comunicarea solicită, de asemenea, investiții în cercetarea științifică și tehnologică pentru a acoperi golurile tehnologice din statele membre. În cele din urmă, comunicarea definește cum să reacționăm la posibilele atacuri informatice din țări terțe. Domeniile prioritare de acțiune ar trebui să fie abuzul sexual asupra minorilor, plăți frauduloase, *botnets* și interferențe neautorizate din cadrul sistemelor informatice.

Având în vedere creșterea exponențială a criminalității informatice din ultimii ani, Parlamentul European a adoptat o rezoluție privind lupta împotriva criminalității informatice la 3 octombrie 2017[31]. Rezoluția „condamnă orice interferență de sistem întreprinsă sau dirijată de o națiune străină sau de agenții săi pentru a perturba procesul democratic dintr-o altă țară". În plus, Parlamentul European subliniază că „gradul de conștientizare cu privire la riscurile prezentate de criminalitatea informatică a crescut, dar măsurile de precauție luate de utilizatori individuali, instituții publice și întreprinderi, rămân complet inadecvate, în principal din cauza lipsei de cunoștințe și resurse".

Rezoluția identifică principalele axe în lupta împotriva criminalității informatice prin evidențierea prevenirii; asigurarea faptului că victimele beneficiază pe deplin de drepturile consacrate în Directiva 2012/29/EU; protecția drepturilor copiilor; consolidarea responsabilității furnizorilor de servicii Internet pentru a obține produse de calitate superioară și mai multă securitate; îmbunătățirea mecanismelor de cooperare între poliție, autoritățile judiciare și furnizorii de servicii de internet; adoptarea unei politici comune privind justiția penală în spațiul informatic, care la rândul său va fi crucială pentru obținerea și păstrarea probelor electronice; consolidarea capacităților informatice și tehnologice; creșterea cooperării cu țările terțe.

Astfel, UE se află într-un proces de modernizare constantă a directivelor sale pentru a se asigura că acestea sunt actualizate pentru a combate în mod eficient noile amenințări. Mai jos sunt enumerate principalele instrumente obligatorii la nivelul UE referitoare la criminalitatea informatică:

În ceea ce privește criminalitatea informatică *strictu sensu*;

Directiva 2011/93 /EU - privind combaterea **abuzului sexual și a exploatării sexuale a copiilor și a pornografiei infantile și înlocuirea Deciziei-cadru 2004/68 /JHA**[32] a Consiliului, care a fost creată pentru a aborda noile fenomene criminale asociate cu abuzul sexual și exploatarea minorilor , grooming și pornografie infantilă online. În acest scop, directiva definește infracțiunile, pedepsele și circumstanțele agravante, precum și pedepsele minime privative de libertate, pedepsirea tentativelor și diferitele forme de autorat, cum ar fi complicitatea și răspunderea penală a persoanelor juridice,

[30] Comunicare comună către Parlamentul European, Consiliul, Comitetul Economic și Social European și Comitetul Regiunilor; Strategia de securitate cibernetică a Uniunii Europene: un spațiu cibernetic deschis, sigur și securizat, Brussels, 7.2.2013, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN .

[31] Rezoluția Parlamentului European din 3 octombrie 2017 privind lupta împotriva criminalității informatice (2017/2068 (INI)), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0366&from=EN.

[32] Directiva 2011/93 /EU a Parlamentului European și a Consiliului din 13 decembrie 2011 privind combaterea abuzului sexual și a exploatării sexuale a copiilor și a pornografiei infantile și care înlocuiește Decizia-cadru a Consiliului 2004/68 /JHA, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN

precum și obligația de a avea baze de date ale infractorilor pentru a preveni recidiva. În cele din urmă, directiva solicită cooperarea între entitățile publice și private în protecția, asistența și sprijinul victimelor și obligația de formare specializată pentru toți cei implicați în proceduri penale. În acest sens, directiva stabilește, de asemenea, garanții procedurale speciale pentru victime, pe lângă cele deja definite în directiva care a stabilit Statutul victimei. În cele din urmă, acesta stabilește existența programelor de intervenție preventivă, măsuri de prevenire și intervenție în timpul sau după procedurile penale. Această legislație a fost transpusă în legislațiile naționale ale statelor membre în 2013. Au fost pregătite deja două rapoarte privind punerea în aplicare a directivei de către statele membre în 2016.

Directiva 2013/40 /EU - **privind atacurile împotriva sistemelor de informații și care înlocuiește Decizia-cadru a Consiliului 2005/222 /JHA**[33] are ca scop reglementarea atacurilor informatice la scară largă, astfel încât statele membre să își consolideze legislația națională în acest domeniu și să definească infracțiunile și sancțiunile pentru infractori precum și răspunderea penală a persoanelor juridice. Directiva vizează, de asemenea, îmbunătățirea cooperării dintre autoritățile competente și statele membre. Această directivă a fost transpusă în sistemele juridice internaționale ale statelor membre în 2015.

Directiva (UE) 2019/713 - **privind combaterea fraudei și contrafacerii mijloacelor de plată fără numerar și care înlocuiește Decizia -cadru 2001/413/JHA**[34] a Consiliului, prezenta directivă este destinată să completeze Directiva 2013/40 /EU pentru a acoperi, ca infracțiuni, conduită digitală care vizează furtul, jaful sau orice altă formă de însușire ilegală, contrafacere sau falsificare, deținerea sau achiziționarea de noi instrumente tehnologice de plată fără numerar, precum și penalitățile minime pentru o astfel de conduită. Prin urmare, această nouă directivă consacră nu numai încălcările legate de instrumentele de plată corporale fără numerar (de exemplu, MBway), ci și necorporale, precum și toate tranzacțiile electronice (de exemplu, tranzacțiile efectuate în monedă virtuală). Astfel, definiția mijloacelor digitale de schimb consacrate în acest document include nu numai mijloacele electronice de plată, ci și, pentru prima dată, mijloacele de plată în monedă virtuală.

Cu privire la obținerea și conservarea dovezilor digitale, în special în legătură cu conținutul ilegal;

Directiva 2000/31 /EC - **privind comerțul electronic**[35]. Printre diversele scopuri ale directivei, le evidențiem pe cele referitoare la furnizorii de servicii. În sensul directivei, activitatea desfășurată de furnizorul de servicii este limitată la procesul tehnic de operare și deschidere a accesului la o rețea de comunicații în care informațiile furnizate de terți sunt transmise sau stocate temporar în singurul scop de a face transmisia mai eficient. Astfel, activitatea furnizorului de servicii este privită ca o activitate pur tehnică, automată și de natură pasivă, ceea ce implică faptul că furnizorul de servicii al societății informaționale nu are cunoștințe sau control asupra informațiilor transmise sau stocate.

În acest sens, Directiva prevede un regim general de iresponsabilitate a furnizorului de servicii pentru conținutul ilegal partajat de utilizatorii serviciului. Astfel, furnizorul de servicii nu are obligația de a monitoriza conținutul și, prin urmare, nu poate fi tras la răspundere pentru acesta. Cu toate acestea, scutirea de răspundere este limitată de obligația de a acționa - prin blocarea sau eliminarea conținutului - atunci când este conștient că destinatarii serviciilor sale îl folosesc pentru a stoca conținut ilegal. În astfel de cazuri, furnizorul

[33] Directiva 2013/40 /EU a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și care înlocuiește Decizia-cadru 2005/222 /JHA a Consiliului, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013L0040&from=EN

[34] Directiva (EU) 2019/713 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind combaterea fraudei și contrafacerii mijloacelor de plată fără numerar și care înlocuiește Decizia-cadru 2001/413/JHA a Consiliului, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L0713&from=EN

[35] Directiva 2000/31 /EC a Parlamentului European și a Consiliului din 8 iunie 2000 privind anumite aspecte juridice ale serviciilor societății informaționale, în special comerțul electronic, pe piața internă („Directiva privind comerțul electronic"),https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

de servicii trebuie, de îndată ce devine conștient sau este informat, să procedeze cu diligență pentru a elimina informațiile sau a dezactiva accesul la acestea. Furnizorul de servicii nu este obligat să monitorizeze în mod activ conținutul ilegal; cu toate acestea, este posibil ca statele membre să definească în lege obligația de îngrijire a furnizorilor de servicii pentru a detecta și preveni anumite tipuri de activități ilegale[36].

Regulamentul 679/2016 - **Implementarea Regulamentului general privind protecția datelor (GDPR)** în 2016[37]. Acest nou cadru legal oferă protecții sporite cu privire la datele cu caracter personal. El exclude din domeniul său de aplicare prelucrarea informațiilor în scopul prevenirii, investigării, depistării sau urmăririi penale de către autoritățile competente[38]. Prin urmare, se aplică tuturor celorlalte situații care implică prelucrarea datelor cu caracter personal, în special la detectarea conținutului ilegal în contextul prelucrării datelor de către un furnizor de servicii sau o altă entitate pe parcursul desfășurării activității lor, deoarece detectarea nu a fost scopul prelucrării datelor. GDPR este încă aplicabil în cazurile în care un organism sau entitate colectează date cu caracter personal în cursul activităților sale și apoi le prelucrează pentru a se conforma unei obligații legale, de exemplu[39] eliminarea conținutului abuzului sexual și exploatarea minorilor sau în cazul instituțiilor financiare atunci când păstrează, în scopul investigării, depistării sau urmăririi penale, anumite date cu caracter personal prelucrate de acestea și furnizează aceste date numai autorităților naționale competente.

Printre diferitele prevederi GDPR, „dreptului de a fi uitat", consacrat în art. 17 din această lege, i se acordă o mai mare importanță în ceea ce privește protejarea drepturilor victimelor, mai ales atunci când datele cu caracter personal sunt prelucrate în mod ilegal și, prin urmare, dau naștere unor prejudicii suplimentare. În acest sens, există cazuri de violență domestică în care imaginile sau videoclipurile intime ale unui partener sunt dezvăluite fără consimțământul partenerului și puse la dispoziție pe un site pornografic. Dreptul la ștergere permite victimei acestei diseminări non-consensuale a videoclipurilor să solicite platformei să elimine imediat conținutul ilegal.

Dreptul de a fi uitat oferă titularului său posibilitatea de **a solicita verbal sau în scris** ca operatorul de date să șteargă datele personale ale persoanei vizate. Circumstanțele în care acest drept poate fi exercitat sunt descrise chiar în articolul 17.

Este important să rețineți că prelucrarea ilegală a datelor cu caracter personal, fie de către responsabilul cu protecția datelor sau de către alte persoane / entități neautorizate să prelucreze aceste date, implică răspundere penală în anumite cazuri[40].

La nivel european, există, de asemenea, instituții care au fost înființate pentru a asista statele membre în combaterea criminalității informatice, cum ar fi Agenția Uniunii Europene pentru securitatea rețelelor și informațiilor (ENISA), care sprijină schimbul de bune practici privind securitatea informatică între statele membre ale UE. Un departament specific pentru combaterea criminalității informatice - Centrul european de criminalitate informatică (EC3) - a fost înființat în cadrul Europol în 2013 pentru a consolida răspunsul autorităților de aplicare a legii din cadrul Uniunii Europene. EC3 acționează oferind sprijin forțelor de poliție ale statelor membre în lupta împotriva criminalității informatice în Uniunea Europeană, reunind experiența

[36] În această privință, consultați, de asemenea: Recomandarea Comisiei (UE) 2018/334 din 1 martie 2018 privind măsurile de combatere eficientă a conținutului ilegal online,https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334&-from=EN.

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

[38] Cf. Art. 2/2/d) GDPRÎn aceste cazuri, se va aplica regimul special al Directivei 2016/680, transpus prin Legea 59/2019.

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

[40] În Portugalia, răspunderea penală în aceste cazuri este prevăzută în Legea 58/2019 din 8 august, articolele 46-52.

lor în sprijinirea investigațiilor privind criminalitatea informatică care ar putea avea loc în statele membre.

În plus față de această inițiativă, Alianța globală împotriva abuzului sexual asupra copiilor online a fost lansată în 2012 de către Comisia Europeană și Statele Unite ale Americii, cu scopul de a reuni eforturile din întreaga lume pentru a combate mai eficient infracțiunile sexuale online împotriva copiilor. Reunind 54 de țări, care s-au angajat să ia măsuri concrete pentru a îmbunătăți protecția victimelor, a identifica și a urmări penal infractorii, a sensibiliza și a reduce răspândirea pornografiei infantile online și a victimizării copiilor.

La nivel internațional, este, de asemenea, important să se sublinieze rolul Asociației INHOPE, a cărei misiune este de a oferi sprijin în crearea și întreținerea de linii de asistență telefonică dedicate combaterii materialelor online de abuz sexual asupra copiilor. Aceste linii telefonice de sprijin acționează la nivel național, în articulație constantă cu omologii lor internaționali, pentru a sprijini structurile care permit societății civile să raporteze conținutul abuzurilor sexuale asupra minorilor care sunt disponibile pe internet. Funcția finală a liniilor telefonice de sprijin este de a duce la eliminarea și responsabilizarea penală a celor care furnizează acest tip de conținut.

2.3. Cadrul legal pentru criminalitatea informatică în unele state membre ale Uniunii Europene

2.3.1. Cazul Portugaliei

În ceea ce privește legislația națională portugheză, cadrul de referință rezultă, în primă instanță, din Legea 109/2009 din 15 septembrie, *Lei do Cibercrime* (LC), Legea privind criminalitatea informatică, care transpune Decizia-cadru 2005/222 /JHA (care a fost înlocuit de Directiva 2013/40 /EU) și adaptează dreptul intern la Convenția de la Budapesta (CCCE).

Această lege prevede așa-numitele infracțiuni informatice strictu sensu, adică acelea a căror practică depinde de un sistem informatic și, sunt prin urmare, *infracțiunile dependente de mediul informatic*. Acest concept de criminalitate informatică se referă la infracțiuni care atacă disponibilitatea, accesul, integritatea, autenticitatea, confidențialitatea, conservarea și securitatea informațiilor.

Cu toate acestea, așa cum vom vedea mai jos, există și alte infracțiuni care pot fi comise folosind mijloace electronice, deși nu exclusiv, făcându-le astfel parte a fenomenului criminalității informatice. În cadrul acestora, există și cele în care legea face trimitere expresă la utilizarea mijloacelor electronice și altele, unde, deși nu există o referință expresă, ele pot fi angajate în continuare folosind tehnologiile informației și comunicațiilor (TIC).

Următoarele tabele analizează tipurile legale de infracțiuni prevăzute la articolele 3-8 din LC:

LEGEA PRIVIND INFRACTIONALITATEA INFORMATICA

Articolul și titlul	Conduita	Natura	Articol al CCCE
Art. 3 - **Falsul computerizat**	Introducerea, modificarea, ștergerea sau suprimarea datelor computerizate cu intenția de a provoca înșelăciunea în raporturile juridice sau de a interfera în alt mod cu prelucrarea datelor computerizate, producând date sau documente false, cu intenția ca acestea să fie considerate sau utilizate în scopurile legale relevante de parcă ar fi adevărate.	Publică	Art. 7
Art. 3, paragraful 3	Utilizarea unui document produs din date de computer care au făcut obiectul actelor menționate la alineatul 1 al acestui articol sau să utilizeze un card sau alt dispozitiv în care datele care au făcut obiectul actelor menționate la alineatul 1 din acest articol sunt înregistrate.		
Art. 4 - **Deteriorarea software-ului sau a altor date ale computerului**	Ștergerea, modificarea, distrugerea, în totalitate sau parțial, deteriorarea, eliminarea sau redarea software-ul inutilizabil sau inaccesibil sau alte date de calculator ale altor persoane sau afectarea în orice fel a capacității lor de utilizare, fără permisiunea legală sau fără a fi autorizat de către proprietar, de către alt titular al dreptului la sistem sau la o parte din acesta.	Semipublic	Art. 7
Art. 4, paragraful 2	Încercarea se pedepsește.		
Art. 5 - **Sabotarea computerului**	Împiedicarea, întreruperea sau perturbarea gravă a funcționării unui sistem informatic prin introducerea, transmiterea, deteriorarea, modificarea, ștergerea, împiedicarea accesului la sau eliminarea software-ului sau a altor date ale computerului sau prin orice altă formă de interferență cu un sistem informatic, fără permisiunea legală sau fără a fi autorizat de proprietar, un alt titular al dreptului sistemului sau o parte din acesta.	Publică	Art. 5
Art. 6 - **Acces ilegal**	Accesarea unui sistem informatic, fără permisiunea legală sau fără a fi autorizat de proprietar, de un alt titular al dreptului sistemului sau a unei părți a acestuia.	Semipublic	Art. 2
Art. 6, n° 5	Încercarea se pedepsește		
Art. 7° - **Interceptarea ilegală**	A intercepta, prin mijloace tehnice, transmisiile de date computerizate care sunt procesate în cadrul unui sistem informatic, direcționate către acest sistem sau pornind de la acesta, fără permisiunea legală sau fără a fi autorizate de către proprietar, de către un alt titular de drept al sistemului sau o parte din acesta .	Publică	Art. 3
Art. 7, paragraful 2	Încercarea se pedepsește.		
Art. 8 - **Reproducerea ilegală a unui program protejat**	Reproducerea, divulgarea sau comunicarea, ilegală, către public, a unuiprogram de computer protejat de lege.	Publică	
Art. 8, paragraful 3	Încercarea se pedepsește.		

LEGEA CRIMINALITĂȚII INFORMATICE- incriminarea comportamentelor de facilitare / sprijin material pentru practicarea conduitei principale ca infracțiuni autonome și nu ca complicitate

Articolul și titlul	Conduita	Articolul CCCE
Articolul 3, paragraful 4 - **Falsul computerizat**	Importarea, distribuirea, vinderea sau deținerea în scopuri comerciale a orice dispozitiv care permite accesul la un sistem informatic, la un sistem de plăți, la un sistem de comunicații sau la un serviciu de acces condiționat, asupra căruia au fost efectuate acțiunile interzise de alineatul 2 al articolului - introducerea, modificarea, ștergerea sau suprimarea de date înregistrate sau încorporate într-un card de plată sau în orice alt dispozitiv care oferă acces la un sistem de plată sau la un mijloc de plată, la un sistem de comunicații sau la un serviciu de acces condiționat, producând date sau documente false; cu intenția ca acestea să fie considerate sau utilizate în scopuri juridice relevante de parcă ar fi adevărate.	Art. 6, **paragraful** 1, als. (a) and (b)
Art. 4(3) - **Deteriorarea software-ului sau a altor date ale computerului**	Producerea, vinderea, distribuirea sau diseminarea sau introducerea în mod ilegal sau introducerea în unul sau mai multe dispozitive de sisteme informatice, software sau alte date de calculator destinate să producă acțiunile neautorizate descrise la alineatul (1) al articolului.	
Articolul 5, paragraful 2 - **Sabotarea computerului**	Producerea, vinderea, distribuirea sau diseminarea sau introducerea în mod ilegal sau introducerea în unul sau mai multe dispozitive de sisteme informatice, software sau alte date de calculator destinate să producă acțiunile neautorizate	
Art. 6, paragraful 2 - **Acces ilegal**	Producerea, vinderea, distribuirea sau diseminarea sau introducerea în mod ilegal sau introducerea în unul sau mai multe dispozitive, programe, sisteme de calculatoare, a unui set de instrucțiuni executabile, cod sau alte date de calculator destinate să producă acțiunile neautorizate descrise la alineatul (1) al articolului.	
Articolul 7, paragraful 3 - **Interceptarea ilegală**	Producerea, vinderea, distribuirea sau diseminarea sau introducerea în mod ilegal sau introducerea în unul sau mai multe dispozitive de sisteme informatice, software sau alte date de calculator destinate să producă acțiunile neautorizate descrise la alineatul (1) al articolului.	

Ar trebui făcute unele considerații cu privire la articolele descrise mai sus.

Articolul 3, privind **falsul computerizat**, urmărește protejarea securității raporturilor juridice ca un interes public esențial, pe care statul de drept trebuie să îl asigure.

Se diferențiază de frauda computerizată, astfel cum este definită la art. 221 din Codul penal portughez, întrucât are drept scop protejarea **binelui legal**. Astfel, în timp ce bunul juridic protejat în primul se referă la integritatea sistemelor de informații și a datelor computerizate, în cel de-al doilea se referă la patrimoniu. În plus, unele conduite tipice care diferă de frauda computerizată, cum ar fi **producerea de date sau documente neautentice cu intenția de a provoca înșelăciune în relațiile juridice și utilizarea documentului ca fiind adevărat**, sunt încă necesare pentru falsificarea computerului.

Trebuie remarcat faptul că paragraful 2 al articolului include falsificarea datelor computerului inserate

în cartelele SIM (Modulul de identitate a abonatului). Acestea sunt carduri de plastic care conțin un cip (structură semiconductoare) pe care sunt stocate informații digitale și care permit titularului să utilizeze un telefon mobil pentru a accesa o rețea de telefonie mobilă. Obiectul comportamentului poate fi, de asemenea, carduri sau alte echipamente care permit accesul la un semnal de televiziune prin cablu, la Internet sau la servicii de telefonie - adică „dispozitive care permit accesul la servicii de acces condiționat".

Exemplu: e-mail de phishing care o redirecționează pe Josefina către o pagină web proiectată de infractori informatici și care arată ca pagina web a băncii sale pentru a o determina pe Josefina să-și plaseze informațiile bancare acolo.

La **articolul 4 - Daune legate de software sau alte date ale computerului**, legiuitorul a intenționat să pedepsească acțiunile ilegale care distrug sau afectează capacitatea de a utiliza software-ul sau datele computerului. Testele de securitate pentru un anumit sistem sunt, prin urmare, excluse, cu condiția să fie autorizate de către proprietarul sistemului respectiv.

Activul legal protejat în acest tip de infracțiuni include integritatea și fiabilitatea datelor și buna funcționare a programelor de computer. Spre deosebire de infracțiunea de prejudiciu definită la art. 212 din Codul penal portughez, articolul 4 nu intenționează doar să protejeze bunurile - daunele computerului. Astfel, pe lângă integritatea patrimonială a datelor computerizate ca proprietate a părții vătămate, acest articol protejează și **integritatea funcțională a datelor** în ceea ce privește **disponibilitatea și utilizarea efectivă a datelor computerizate**. Nu necesită o intenție specifică.

Exemplu: computerul lui João este infectat cu un virus care face computerul său foarte lent.

Articolul 5 - Sabotajul computerului are drept scop protejarea împotriva **întreruperii sistemelor informatice sau a comunicării datelor**.

Distincția dintre deteriorarea computerului și sabotajul computerului nu este ușoară. Comparând cele două tipuri de infracțiuni, putem spune că articolul despre avariile computerului intenționează să pedepsească faptele legate de **datele computerului**, în timp ce articolul despre **sabotaj pedepsește întreruperea funcționării normale a sistemelor informatice**. Din punct de vedere individual, putem avea acte de deteriorare a computerului care au, ca rezultat practic, sabotarea computerului datorită impactului lor asupra funcționării unui sistem computerizat sau asupra comunicării datelor. În acest caz, **pagubele sunt doar forme ale infracțiunii de sabotaj pe computer**. Cu alte cuvinte, sabotarea computerului va duce întotdeauna la deteriorarea computerului.

Dispoziția sancționează, de asemenea, răspândirea virușilor și a altor programe rău intenționate concepute pentru a provoca sabotarea computerelor (de exemplu, art. 5, alin. 2 din LC). În aceste cazuri, criminalizăm faza pregătitoare a actelor de sabotaj, de exemplu, asamblarea rețelelor de bots destinate să permită controlul malefic al rețelelor, prin înființarea unei rețele de calculatoare zombie a

cărei utilizare ulterioară va provoca defecțiuni tehnice cunoscute sub numele de DoS și DDoS.

Articolul 6 - Accesul ilegal are drept scop protejarea securității sistemului informatic și a confidențialității acestuia. Aceasta este o infracțiune abstractă de pericol menită să acționeze ca o barieră pentru a preveni comiterea altor infracțiuni mai grave. Prin urmare, pentru ca comportamentul tipic să apară, este suficient ca **accesul neautorizat să fie finalizat**, întrucât cunoașterea secretelor comerciale sau industriale sau a datelor confidențiale, protejate de lege, constituie o circumstanță agravantă a infracțiunii de acces ilegal (art. 6, nr. 4 din LC).

Nu este necesară deteriorarea sau pierderea datelor, programelor sau sistemelor informatice pentru a consuma infracțiunea de acces ilegal. În sensul legii, accesul este intrarea în tot sau în parte a unui sistem informatic (hardware, componente, date stocate în sistem, fișiere, date despre trafic și date referitoare la conținut). Cu toate acestea, art. 6.2 nu pedepsește achiziționarea / cumpărarea de date sau programe care facilitează accesul, ci doar vânzarea.

Pentru ca infracțiunea să fie consumată, făptuitorului nu i se cere să aibă vreo intenție specifică, este suficient ca aceștia să aibă intenția de a accesa sistemul.

Exemplu: infracțiunea de acces ilegal este comisă de cineva care nu este autorizat să acceseze un grup privat de pe rețeaua socială WhatsApp creată de studenți în anul 7.

La **articolul 7 - Interceptarea ilegală**, legea intenționa să protejeze dreptul la confidențialitate, ca un drept la secret asupra comunicărilor datelor computerizate, prin secret în toate comunicațiile digitale.

Interceptare autorizată prin lege (desfășurată în conformitate cu normele procesuale penale, de exemplu: art. 12-19 din LC) sau efectuată cu autorizarea sau prin ordin al celor implicați în transmiterea datelor (activități de testare sau protecție aprobate de participanți)) sunt excluse din această tipificare penală.

Este o infracțiune interceptarea oricărei forme de transfer electronic de date, prin telefon, fax, e-mail sau fișier. Pentru desăvârșirea infracțiunii **nu este necesar să se obțină în mod eficient informații**, este suficient să se acționeze cu obiectivul de a captura aceste informații, deoarece încercarea de interceptare este pedepsită.

Termenul „nepublic" stabilește natura comunicării și nu natura datelor transmise. Datele comunicate pot constitui informații disponibile publicului, dar părțile ar putea dori să comunice cu încredere; sau datele pot fi păstrate confidențiale în scopuri comerciale până când serviciul este remunerat. Astfel, termenul „non-public" nu exclude rețelele publice.

Exemplu: Pedro instalează software pe telefonul Mariei care îi permite să aibă acces la toate comunicațiile sale telefonice.

Trebuie remarcat faptul că tipurile de infracțiuni prevăzute la articolele 3-7 includ, de asemenea, cu aceleași pedepse, actele de producere, vânzare, distribuire, diseminare sau introducere într-un sistem informatic a unui dispozitiv sau program care permite practicarea conduitei tipificate pentru infracțiunea în cauză. De exemplu: În cazul accesului ilegal, agentul infracțiunii de acces ilegal este autorul (autorii) programului care permite unei terțe părți să acceseze sistemul altei persoane, chiar dacă nu au accesat sau au încercat să îl acceseze.

Articolul 8 - Reproducerea ilegală a unui program protejat are drept scop protejarea unui drept privat, a unui program de computer. În acest sens, articolul 14 din DL 252/94, din 20/10, care reglementează protecția legală a programelor de calculator, prevede în mod expres că prevederile articolului 9 (1) din LC sunt aplicabile programelor de computer. Astfel s-a înțeles că există un interes esențial al statului în **protejarea drepturilor intelectuale ale creatorilor** și că, prin urmare, interesul statului de a acționa penal împotriva încălcării drepturilor de această natură era justificat. Prin urmare, această infracțiune nu depinde de plângere, fiind o infracțiune publică.

Articolele 11-19 stabilesc reguli privind dreptul procesual, care permit colectarea și menținerea rapidă a probelor electronice. Prin urmare, acestea se aplică infracțiunilor prevăzute în prezenta lege, celor comise prin intermediul unui sistem informatic sau celor care necesită colectarea probelor în formă electronică.

Articolele 20-26 se referă la cooperarea internațională și articolul 27 la jurisdicția teritorială.

Codul penal portughez și dispozițiile privind criminalitatea informatică

După cum sa menționat anterior, în sistemul juridic portughez, pe lângă LC, este posibil să se găsească infracțiuni definite care pot fi săvârșite prin mijloace electronice, deși nu exclusiv, numite și infracțiuni de tip *cyber-enabled* (facilitate informatic).

În unele cazuri, legea prevede în mod expres utilizarea acestor mijloace electronice, în altele nu. În Codul penal în sine pot fi găsite unele dispoziții care se referă în mod expres la utilizarea mijloacelor electronice pentru a comite infracțiunea. Următorul tabel reunește dispozițiile referitoare la infracțiunile cu activități informatice:

CODUL PENAL PORTUGHEZ

Articol și titlu	Condutas	Natureza
Articolul 152, paragraful 2, al. b) – **Violența domestică**	Diseminarea datelor cu caracter personal, precum imagini sau sunete, referitoare la confidențialitatea uneia dintre victime fără consimțământul acestora, prin internet sau prin alte mijloace de diseminare publică generală.	Public
Art. 176, paragraful 1, als. a), b), c) and d) – **Pornografia minorilor**	Folosirea unui minor într-o emisiune pornografică sau atragerea lor în acest scop; folosirea unui minor într-o fotografie, film sau înregistrare pornografică sau, indiferent de suport, atragerea lor în acest scop; producerea, distribuirea, importul, exportul, divulgarea, expunerea, oferirea sau punerea la dispoziție materialele prevăzute în paragraful anterior; achiziționarea, deținerea sau găzduirea acelor materiale cu scopul de a le distribui, importa, exporta, divulga, expune sau dărui.	Public
Art. 176, no. 5	Să achiziționeze, să dețină, să acceseze, să obțină sau să faciliteze accesul prin intermediul sistemului informatic sau prin orice alt mijloc la materialele menționate la litera (b).	
Art. 176, no. 6	În persoană sau printr-un sistem informatic sau orice alt mijloc, să participe, să faciliteze sau să pună la dispoziție accesul la o emisiune pornografică care implică participarea minorilor sub 16 ani.	
Art. 176, no. 8[41]	Încercarea se pedepsește.	
Art. 176 - A – **Grooming-ul minorilor**	Grooming-ul minorilor, prin intermediul tehnologiilor informaționale și de comunicare, pentru întâlniri care vizează practicarea actelor de abuz sexual al minorilor sau a actelor de pornografie infantilă.	Public
Art. 193 - **Intruziune prin intermediul TIC**	Să creeze, să întrețină sau să utilizeze un fișier cu date identificabile individual referitoare la credințe politice, religioase sau filosofice, apartenență la partid sau sindicat, viață privată sau origine etnică.	Public
Art. 193, paragraph 2	Încercarea se pedepsește.	
Art. 221 - **Fraude informatice și de comunicații**	Interferența cu rezultatul prelucrării datelor sau structurarea incorectă a unui program de computer, utilizarea datelor incomplete sau incorecte, utilizarea datelor sau intervenirea în orice mod în prelucrare, fără autorizație, cu intenția de a obține pentru sine sau pentru o terță parte o îmbogățire nedreaptă, provocând cealaltă persoană prejudiciu patrimonial.	Semipublic
Art. 221, paragraful 2	A provoca daune proprietății altora, folosind programe, dispozitive electronice sau alte mijloace care, separat sau împreună, sunt menite să diminueze, să modifice sau să împiedice, în totalitate sau parțial, funcționarea normală sau funcționarea serviciilor de telecomunicații.	
Art. 221, paragraful 3	Încercarea se pedepsește.	

[41] Noul nr. 8 al articolului 176 din versiunea proiectului de lege nr. 187 / XIV / 1 adaugă o definiție a „materialului pornografic", ca orice material care, în scopuri sexuale, reprezintă minori implicați într-un comportament sexual explicit sau real sau conține orice reprezentare a organelor lor sexuale sau a altei părți a corpului lor.

Crimes que, pesa embora não exista menção expressa de recurso a meios eletrónicos, são hoje em dia, maioritariamente, praticados por via daqueles;

Art. 154a - Persecutarea	Să persecute sau să hărțuiască o altă persoană, prin orice mijloace, direct sau indirect, în mod repetat, într-un mod care să provoace frică sau neliniște sau să le afecteze libertatea de judecată.	Semipublic
Art. 154a , paragraful 2	Încercarea se pedepsește.	
Art. 192 – **Intruziune în confidențialitate**	A intercepta, înregistra, utiliza, transmite sau divulga o conversație, o comunicare telefonică, mesaje de e-mail sau facturare detaliată; să surprindă, să fotografieze, să filmeze, să înregistreze sau să divulge imagini ale unor persoane sau ale unor obiecte sau spații intime; să observe sau să asculte, ascuns, persoanele care se află într-un loc privat sau să dezvăluie fapte legate de viața privată a victimei sau de boala gravă, fără consimțământul victimei și cu intenția de a pătrunde în viața privată a victimei, în special în familia lor sau intimitate sexuală.	Semipublic
Articolul 194 - **Încălcarea corespondenței sau a telecomunicațiilor**	să deschidă un colet, o scrisoare sau orice altă scrisură care este închisă și care nu se adresează propriei persoane, sau să devină conștient, prin procese tehnice, de conținutul său sau să împiedice, în vreun fel, să fie primite de către destinatar; interferarea cu conținutul telecomunicațiilor sau conștientizarea acestora și dezvăluirea conținutului scrierilor închise sau al telecomunicațiilor.	Semipublic
Articolul 199 - Înregistrări și fotografii ilicite	Să înregistreze, fără consimțământ, cuvintele rostite de o altă persoană și care nu sunt destinate publicului, chiar dacă le sunt adresate; să utilizeze sau să permită utilizarea unor astfel de înregistrări chiar dacă sunt produse în mod legal; să fotografieze sau să filmeze o altă persoană, chiar la evenimente la care au participat în mod legal sau să utilizeze sau să permită utilizarea acestor fotografii sau filme deja menționate, chiar dacă au fost obținute în mod legal.	Semipublic
Art. 199, paragraful 2, b)	Divulgarea imaginilor neautorizate.	
Art. 240(1)(a) și (b) - **Discriminarea și incitarea la ură și violență**	Să înființeze sau să constituie o organizație sau să se angajeze în activități de propagandă organizată care să incite sau să încurajeze discriminarea, ura sau violența împotriva persoanelor sau grupurilor de persoane din cauza rasei, culorii, originii lor etnice sau naționale, strămoșilor, religiei, sexului, orientării sexuale, identității de gen sau dizabilitate fizică sau psihică; sau să participe sau să ofere asistență organizației sau activităților menționate la paragraful precedent, inclusiv finanțarea.	Public
Art. 240, para. 2, al) a	Prin justificarea, negarea sau banalizarea gravă a crimelor de genocid, război sau împotriva păcii și umanității, în mod public, prin orice mijloace destinate publicității, provocării actelor de violență, defăimării sau insultei, amenințării sau incitării la violență sau ură, împotriva persoanelor menționate la paragraful 1.	

Dispoziția din **articolul 152 alineatul (2) litera (b) - Violența în familie** a fost introdusă prin Legea 44/2018. Acest nou precept își propune să protejeze datele personale (și anume imaginea sau sunetul, care includ videoclipuri, filme, fotografii) cu privire la intimitate (și anume sexualitatea) în special cu privire și la confidențialitatea oricărei victime atunci când este difuzată (postată / răspândită) prin intermediul internetului sau prin alte diseminare publică pe scară largă (cum ar fi prin intermediul rețelelor sociale),

fără acordul victimei. Această criminalizare a avut ca scop penalizarea în continuare, prin această calificare specială, a stalking-ului informatic în cadrul violenței domestice (înțeleasă ca o conduită constând în principal, potrivit Carolina Villacampa Estiarte, în „trimiterea de mesaje e-mail ofensive sau amenințătoare, mesaje text și mesaje instantanee, publicarea de comentarii jignitoare despre victimă pe Internet, schimbul de fotografii sau videoclipuri intime ale victimei prin intermediul internetului, care sunt experimentate ca „mai intruzive pentru victime" și care „le provoacă efecte psihologice mai negative").

În ceea ce privește **articolul 176 - Pornografia minorilor**, actele materiale enumerate depășesc cele descrise în Directiva 2011/93/EU, deși nu sunt la fel de avansate ca Convenția de la Lanzarote. În acest sens, trebuie remarcat faptul că Proiectul de lege nr. 187 / XIV / 1 a modificat unele paragrafe ale acestui articol (a se vedea nota de subsol la tabel) și a adăugat, de asemenea, articolul 176-B privind organizarea de excursii în scopuri de turism sexual cu minori în Codul penal[42].

Articolul 176 - Ademenirea minorilor în scopuri sexuale a fost adăugat la Codul penal prin Legea nr. 103/2015, din 24 august. Astfel, respectând prevederile Directivei 2011/93 / EU, noi forme de abuz sexual și exploatare facilitate de utilizarea TIC, cum ar fi, de exemplu, grooming-ul minorilor prin intermediul internetului, spectacole pornografice în timp real pe internet sau accesarea cu bună știință și intenționată a pornografiei infantile găzduite pe anumite site-uri de internet, au devenit criminalizate.

Articolul 193 - Intruziunea prin intermediul TIC, derivă din preceptul constituțional prevăzut la articolul 35 alineatul (3) din Constituția Republicii Portugheze. Acesta își propune să protejeze rezerva de confidențialitate împotriva unor eventuale acte de discriminare, făcute exponențial periculoase prin utilizarea mijloacelor computerizate. Acesta este motivul pentru care procedura penală în legătură cu infracțiunea prevăzută în acest articol 193 nu depinde de o plângere. Este astfel o infracțiune publică, asupra căreia statul va avea întotdeauna interesul și datoria de a acționa. În infracțiunea de intruziune prin intermediul TIC, găsim nu numai faptele de creare a unor fișiere care încalcă fișierele proprietății protejate, ci și simplele acte de păstrare și utilizare a fișierului, chiar dacă fără o coparticipare la crearea acestuia. Definiția infracțiunii este, așadar, destul de cuprinzătoare în ceea ce privește conduita sancționată și se dorește a fi un factor de descurajare, având în vedere dificultatea de a dovedi cine este autorul material al dosarului. În același sens, simpla încercare este penalizată.

Incriminarea **fraudei și a comunicațiilor informatice** prevăzută la **articolul 221** este aliniată la evoluțiile din domeniul general al fraudei, împărtășind aceleași elemente definitorii ale infracțiunii descrise la articolul 217 din Codul de procedură penală - intenția de a obține pentru sine, sau pentru o terță parte, îmbogățirea ilegală și provocarea de daune patrimoniale unei terțe părți. Ca și în cazul infracțiunii generice de înșelăciune, tentativa este pedepsită, iar procedura penală depinde de o plângere. **Specificitatea acestei infracțiuni** constă în procesul folosit: **utilizarea mijloacelor TIC**, adică utilizarea mijloacelor computerizate într-un mod viclean pentru a manipula date sau rezultate. Paragraful 1 al articolului se referă la interferența cu rezultatul prelucrării datelor care vizează obținerea unui avantaj ilegal, în timp ce paragraful 2 se referă la utilizarea TIC menită să perturbe integritatea / funcționarea normală a sistemelor informatice pentru a obține un avantaj ilegal.

[42] Până la data publicării acestui manual, proiectul de lege menționat va fi fost deja aprobat în Parlament, trimis spre promulgare, lipsind doar publicarea acestuia. Prin urmare, modificările sunt admise ca fiind sigure, dar nu este posibil să se specifice numele / numărul final al Legii. Cf.. https://www.parlamento.pt/ActividadeParlamentar/Paginas/DetalheIniciativa.aspx?BID=44369

Acum este necesar să se analizeze preceptele care se referă la infracțiuni care, deși nu prevăd în mod expres utilizarea mijloacelor TIC, au o mare probabilitate de utilizare a acestor mijloace, având în vedere creșterea exponențială a accesului la internet și smartphone-uri.

Articolul 194 - Încălcarea corespondenței sau a telecomunicațiilor, infracțiunea este agravată dacă conținutul este difuzat prin internet (cf. art. 197 CP). Acest articol derivă din dreptul fundamental prevăzut la articolul 34 din Constituția portugheză, care consacră secretul comunicărilor, definind încălcarea acestuia ca fiind o infracțiune. Se aplică direct corespondenței electronice (prin e-mail) și tuturor celorlalte servicii de comunicații electronice și de telefonie mobilă (SMS etc.) care sunt comparabile în era modern cu corespondența poștală sigilată. Activele protejate în acest precept sunt confidențialitatea, protecția libertății de exprimare și încrederea comunității în integritatea mijloacelor de comunicare, și anume telecomunicațiile și securitatea.

Se asigură protecție atât conținutului comunicațiilor electronice, cât și circumstanțelor comunicării (date despre trafic). Simpla păstrare a datelor este o încălcare, care se repetă în fiecare nouă utilizare sau utilizare a conținutului datelor de trafic. În comunicațiile electronice, pentru ca infracțiunea să apară, nu este necesar să se cunoască conținutul, accesul este suficient (în telecomunicații nu este necesar să se „deschidă").

Se pune întrebarea dacă această infracțiune nu este absorbită de infracțiunea de „interceptare ilegală" prevăzută de articolul 7 din Legea 109/91. Ni se pare că, deși poate exista o suprapunere atunci când mesajul este interceptat în timpul transmiterii sale, acest lucru nu va mai fi cazul atunci când mesajul este accesat după ce a fost deja primit de către destinatar și este stocat în fișierul său electronic. cutie poștală. Deși, în acest din urmă caz, s-ar putea spune, de asemenea, că aceasta este o infracțiune de „acces ilegal" prevăzută de articolul 6 din LC, credem că acest lucru nu este cazul, în primul rând deoarece această infracțiune **necesită o intenție specială : „intenția de a obține, pentru dvs. sau pentru alții, un beneficiu sau un avantaj ilegal"**, pe care infracțiunea „încălcării corespondenței sau telecomunicațiilor" nu o impune. Prin urmare, nu s-ar justifica faptul că o poștă electronică închisă, odată primită, ar fi mai puțin protejată decât poșta de hârtie. Prin urmare, înțelegem că această infracțiune se aplică în continuare poștei electronice.

Încă sub incidența protecției vieții private sau a confidențialității, avem următoarele infracțiuni: **invazia domiciliului sau încălcarea vieții private** (art. 190 Cod penal), **încălcarea într-un loc închis publicului** (191 PC), **încălcarea dreptului la viața privată** (art. 192 PC), **încălcarea secretului** (art. 195 PC). În toate acestea, se prevede o agravare dacă conținutul este difuzat prin internet, cf. art. 197 PC).

Dispoziția privind **fotografiile și înregistrarea ilicite** prevăzute la **art. 199 din Codul penal portughez** intenționează să protejeze dreptul de a proteja propria imagine, care este un activ juridic și penal autonom protejat în sine și independent din punctul de vedere al confidențialității sau intimității prezentate. Dreptul la propria imagine acoperă două drepturi autonome: dreptul de a nu fi fotografiat și dreptul de a nu fi publicată fotografia. Persoana în cauză poate autoriza sau consimți să

fie fotografiată și poate să nu autorizeze utilizarea sau publicarea acelei fotografii. Subiectul nu poate fi fotografiat sau fotografia sa utilizată împotriva voinței sale.

Exemplu: João, împotriva voinței Mariei, îi folosește fotografia, obținută legal - Maria a consimțit să fie fotografiată - și o publică pe *Facebook*.

Pe lângă acestea, pot fi comise și alte infracțiuni comune, iar efectele lor pot fi îmbunătățite prin utilizarea tehnologiilor. **Acestea sunt infracțiuni a căror tipologie nu consideră utilizarea tehnologiei ca un element constitutiv al infracțiunii**.

Stalking-ul, definit la **art. 154-A**, poate fi comis prin mijloace electronice: stalking-ul informatic. Tinde să apară pe perioade lungi de timp, cu consecințe, în multe cazuri, devenind mai grave în timp. Datorită acestui fapt, infracțiunea de urmărire poate integra alte tipuri de infracțiuni, de ex. art. 193 CP, care definește intruziunea prin mijloace TIC, înregistrarea infracțiunilor și fotografiile ilicite prevăzute la art. 199 CP[43]. De asemenea, infracțiunea de **discriminare și incitare la ură și violență**, prevăzută la **articolul 240**, poate fi comisă prin mijloace electronice.

Alte exemple:

Infracțiuni împotriva onoarei comise prin includerea unor expresii sau acuzații jignitoare în pagini online, bloguri sau diseminarea lor prin e-mail. Suportul electronic este relevant deoarece este utilizat pentru divulgarea conținutului insultător sau defăimător și are un potențial mai mare de a afecta bunul juridic protejat (cf. Art. 183/1 a) PC: infracțiune practicată prin mijloace care facilitează diseminarea acestuia ; si nr. 3 PC: suport de comunicare în masă, de ex. retele sociale).

Decretul-lege nr. 7/2004 din 7 ianuarie a transpus Directiva 2000/31/EC. Astfel, acest instrument stabilește principiul iresponsabilității furnizorilor intermediari de servicii de rețea în fața unei posibile ilegalități a mesajelor pe care le pun la dispoziție. În acest sens, se abate de la absența unei obligații generale de vigilență din partea furnizorului de servicii intermediare cu privire la informațiile pe care le transmite sau le stochează sau la care oferă acces (art. 12), la obligația de informare / comunicare imediată Parchetului ori de câte ori sunt conștienți de faptul că furnizarea de conținut prin serviciile pe care le furnizează sau accesul la acestea poate constitui o infracțiune (art. 13 a). Cea mai recentă modificare introdusă prin Proiectul de lege nr. 187 / XIV / 1 extinde această obligație de informare și o întărește în raport cu orice caz de detectare a conținutului pus la dispoziție de către furnizorul de servicii care poate constitui o infracțiune, și anume infracțiunea de pornografie a minorilor sau infracțiunea de discriminare și incitare la ură și violență[44].

În plus față de această obligație de a notifica autoritățile, furnizorii de servicii intermediare sunt responsabili, de asemenea, în cazurile în care devin conștienți - ei înșiși sau prin terțe părți - de existența unui conținut cu caracter **vădit** ilegal, pentru blocarea sau eliminarea acestuia (cf. art. 13 c); artă. 15, alin. 3; artă. 16, alin. 1; artă. 17). Odată cu modificările introduse prin Proiectul de lege nr. 187

[43] Cibercrime and Stalking, Vânia Costa Ramos, p. 11. https://carlospintode-abreu.com/public/files/cibercrime_stalking.pdf

[44] Consultați noul articol 19-A din Decretul-lege nr. 7/2004, adăugat după aprobarea Proiectului de lege nr. 187 / XIV.

/ XIV / 1, Furnizorii sunt obligați să elimine, în termen de 48 de ore, conținutul referitor la abuzul sexual sau exploatarea minorilor[45].

Nerespectarea obligațiilor specifice de informare și blocare determină răspunderea furnizorilor de servicii intermediare, fie prin mecanismul de răspundere civilă (art. 16), fie prin aplicarea infracțiunilor administrative (art. 37) de către entitatea responsabilă pentru supraveghere - ANACOM.

Legea 32/2008 din 17 iulie 2008, cunoscută sub numele de Legea privind păstrarea datelor (în portugheză Lei de Retenção de Dados, LRD) în contextul furnizării de servicii de comunicații electronice pentru investigarea, depistarea și urmărirea penală a infracțiunilor grave de către autoritățile competente. A transpus Directiva 2006/24 /EC, care nu mai este în vigoare în legislația UE[46]. Cu toate acestea, această lege este încă în vigoare în sistemul juridic portughez. Cele mai relevante dispoziții privind conservarea dovezilor digitale pot fi găsite în articolul 4, paragraful 3, care definește care sunt infracțiunile grave în sensul prezentei legi, prezentând astfel un catalog al infracțiunilor a căror anchetă va permite utilizarea datelor reținute de către serviciu furnizorii și articolul 6, care prevede **o perioadă de un an pentru stocarea datelor de trafic și de localizare** în sectorul comunicațiilor electronice.

În cele din urmă, **Legea 46/2018 din 13 august** stabilește **cadrul legal pentru securitatea spațiului informatic** (în portugheză, Regime Jurídico da Segurança do Ciberespaço) și transpune Directiva (UE) 2016/1148 privind măsurile pentru asigurarea unui nivel comun ridicat de securitate a rețelelor și a informațiilor în întreaga Uniune[47]. Acesta a creat Consiliul superior de securitate informatică (în portugheză Conselho Superior de Segurança do Ciberespaço CSSC), ca organism specific consultat de prim-ministru cu privire la chestiuni legate de securitatea spațiului informatic. În articolele 5 și 6 legea definește competențele CSSC, iar în articolul 7 definește competențele Centrului național de securitate informatică (în portugheză, Centro Nacional de Cibersegurança CNCS). În articolele 8 și 9, legea oferă cadrul legal pentru Echipa Națională de Răspuns la Incidente de Securitate a Computerelor - în portugheză Equipa de Resposta a Incidentes de Segurança Informática Nacional CERT.PT - și definește competențele sale, integrate în CNSC. Această lege stabilește, de asemenea, cerințele minime de securitate informatică și obligațiile de raportare a incidentelor la toate nivelurile guvernamentale și entitățile publice, furnizorii de servicii de infrastructură critică, operatorii de servicii esențiale și furnizorii de servicii digitale, față de CNCS, care ulterior informează, dacă este necesar, punctele de contact ale altor state membre afectate.

La 12 iunie 2019, Guvernul a adoptat **Rezoluția Consiliului de Miniștri nr. 92/2019 care a aprobat prima strategie națională pentru securitatea spațiului informatic**, cu scopul de a îmbunătăți securitatea rețelelor și a sistemelor de informații și de a spori utilizarea gratuită, sigură și eficientă a spațiului informatic de către toți cetățenii și entitățile publice și private. Strategia se bazează pe trei principii: subsidiaritatea intervenției statului, complementaritatea acțiunii (strânsă legătură și coordonare cu diferiți actori) și proporționalitatea (în alocarea resurselor și serviciilor pentru a face față amenințărilor digitale).

[45] Vezi articolul 19 B din Decretul-lege nr. 7/2004, adăugat după aprobarea Proiectului de lege nr. 187 / XIV / 1, care impune în mod expres eliminarea, în termen de 48 de ore, a conținutului abuzurilor sau exploatării sexuale a minorilor.

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

[47] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru a asigura un nivel comun ridicat de securitate a rețelelor și informațiilor în întreaga Uniune.https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=PT

2.3.2. Cazul României

Sistemul juridic românesc nu are o lege specială privind criminalitatea informatică. În acest sens, prevederile legale pentru acest tip de infracțiuni sunt prevăzute în Codul penal român sub două titluri diferite:

Titlul II - Infracțiuni contra patrimoniului
Capitolul IV - Fraude comise prin sisteme informatice și mijloace de plată electronice

- **Frauda informatică** (Art. 249), definită ca fiind „Introducerea, modificarea sau ștergerea de date informatice, restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane";
- **Efectuarea de operațiuni financiare în mod fraudulos** (Art. 250) - „(1) Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia", respectiv „(3) Transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute în alin. (1)";
- **Acceptarea operațiunilor financiare efectuate în mod fraudulos** (Art. 251) - „Acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său";

Titlul VII - Infracțiuni contra siguranței publice
Capitolul VI - Infracțiuni contra siguranței și integrității sistemelor și datelor informatice

- **Accesul ilegal la un sistem informatic** (Art. 360), care diferențiază între accesul ilegal la un sistem informatic, accesul ilegal la un sistem informatic în scopul obținerii datelor computerizate și accesul ilegal la un sistem informatic care are programe, dispozitive sau proceduri care restricționează accesul la acesta. Cele trei tipuri de infracțiuni corespund unor pedepse din ce în ce mai severe;
- **Interceptarea ilegală a unei transmisii de date informatice** (Art. 361), definită ca „(1) Interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic", respectiv „(2) interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice.";
- **Alterarea integrității datelor informatice** (Art. 362) - „Fapta de a modifica, șterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept";
- **Perturbarea funcționării sistemelor informatice** (Art. 363) - „Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice";

- **Transferul neautorizat de date informatice** (Art. 364) – „Transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice";
- **Operațiuni ilegale cu dispozitive sau programe informatice** (Art. 365) - „(1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă: a) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364; b) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364", respectiv „(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364".

Título VIII – Crimes que afetam relações de coexistência social
Capítulo I – Crimes contra a paz e a ordem pública

- **Pornografia infantilă** (Art. 374), definită ca fiind „producerea, deținerea, obținerea, conservarea, expunerea, promovarea, difuzarea sau divulgarea și / sau furnizarea în orice mod a conținutului pornografic cu minori, precum și a extorcării sau recrutării minorilor în scopul participării la o emisiune pornografică, obținând astfel un avantaj sau exploatând în alt mod minorii în scopul realizării unui spectacol pornografic ". Vizualizarea conținutului pornografic referitor la minori este, de asemenea, pedepsită prin lege. Componenta criminalității informatice în pornografia infantilă este evidentă la articolul 374, paragraful 2, în partea în care menționează în mod expres sancțiunile pentru comportamentele menționate mai sus, fie că au fost comise prin intermediul unui sistem informatic sau prin orice alt mijloc de comunicare electronică. În plus, paragraful 4 include în mod expres noile tehnologii de informare și comunicare ca mijloace de comunicare pentru spectacole pornografice.

Tentativa de a comite oricare dintre comportamentele de mai sus se pedepsește în conformitate cu articolele 252, 366 și 374 (5) din Codul penal român.

„(1) Producerea, deținerea, procurarea, stocarea, expunerea, promovarea, distribuirea, precum și punerea la dispoziție, în orice mod, de materiale pornografice cu minori", inclusiv „(1^1) îndemnarea sau recrutarea unui minor în scopul participării lui în cadrul unui spectacol pornografic, obținerea de foloase de pe urma unui astfel de spectacol în cadrul căruia participă minori sau exploatarea unui minor în orice alt fel pentru realizarea de spectacole pornografice". De asemenea, este interzisă „(1^2) Vizionarea de spectacole pornografice în cadrul cărora participă minori". Apoi, „(2) Dacă faptele prevăzute în alin. (1) au fost săvârşite printr-un sistem informatic sau alt mijloc de stocare a datelor informatice" pedeapsa se majorează (închisoare de la 2 la 7 ani). Articolul include și „(3) Accesarea, fără drept, de materiale pornografice cu minori, prin intermediul sistemelor informatice sau altor mijloace de comunicaţii electronice".

Majorarea pedepsei în cazul pornografiei infantile se face în următoarele situații:

„(3^1) Dacă faptele prevăzute la alin. (1), (1^1), (1^2) și (2) au fost săvârșite în următoarele împrejurări:

a. de către un membru de familie;

b. de către o persoană în a cărei îngrijire, ocrotire, educare, pază sau tratament se afla minorul sau de o persoană care a abuzat de poziția sa recunoscută de încredere sau de autoritate asupra minorului;

c. fapta a pus în pericol viața minorului, limitele speciale ale pedepselor se majorează cu o treime."

Alte definiții relevante din cadrul articolul 374 sunt:

„(4) Prin *materiale pornografice* cu minori se înțelege orice material care prezintă un minor ori o persoană majoră drept un minor, având un comportament sexual explicit sau care, deși nu prezintă o persoană reală, simulează, în mod credibil, un minor având un astfel de comportament, precum și orice reprezentare a organelor genitale ale unui copil cu scop sexual.

(4^1) Prin *spectacol pornografic* se înțelege expunerea în direct adresată unui public, inclusiv prin tehnologia informațiilor și comunicațiilor, a unui copil implicat într-un comportament sexual explicit ori a organelor genitale ale unui copil, cu scop sexual."

Angajamentul țării de a combate criminalitatea informatică a fost consolidat în 2011, când guvernul a creat *Centrul Național de Răspuns la Incidente de Securitate Cibernetică* - CERT-RO, care constă dintr-un centru independent și specializat de cercetare și dezvoltarea în securitatea cibernetică. În 2013, România a aprobat *Strategia națională pentru securitate cibernetică*, care vizează, de asemenea, crearea unui sistem național de securitate cibernetică (în limba română: Sistemul național de securitate cibernetică - SNSC), care se bazează pe un cadru general pentru cooperarea intersectorială între autoritățile publice și instituții sau reprezentanți ai industriei.

În iulie 2020, Legea 217/2003 privind prevenirea și combaterea violenței domestice a fost modificată și **violența cibernetică** a fost inclusă printre formele recunoscute de violență domestică, alături de violența verbală, fizică, sexuală, psihologică, economică, spirituală și socială. Conform Legii 217/2003, violența cibernetică este definită ca „hărțuire online, mesaje online instigatoare la ură pe bază de gen, urmărire online, amenințări online, publicarea nonconsensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima" (Art. 4, lit. h). Este important de

reținut că aceste dispoziții se referă la „orice inacțiune sau acțiune intenționată de violență fizică, sexuală, psihologică, economică, socială, spirituală sau cibernetică, care se produce în mediul familial sau domestic ori între soți sau foști soți, precum și între actuali sau foști parteneri, indiferent dacă agresorul locuiește sau a locuit împreună cu victima" (Art. 3).

În cele din urmă, la momentul finalizării acestui manual, o propunere de sancționare a **pornografiei non-consensuale** (sau așa-numita „pornografie de răzbunare", „revenge porn"), adoptată de Senat la 21 octombrie 2019 și trimisă ulterior Camerei Deputaților pentru dezbatere, era în curs de examinare în Parlamentul României. Propunerea urmărește modificarea articolului 226 din Codul penal (care reglementează infracțiunea de violare a vieții private) pentru a include infracțiunea de pornografie non-consensuală. Propunerea de modificare are următorul conținut:

„După alineatul (5) al art. 226 se introduc 4 noi alineate, cu următorul cuprins:

(6) Divulgarea, difuzarea, prezentarea sau transmiterea, în orice mod, a unei imagini intime a unei persoane identificate sau identificabile după informațiile furnizate, fără consimțământul persoanei înfățișate, de natură să provoace acesteia o suferință psihică sau o știrbire a imaginii sale, se pedepseşte cu închisoare de la 3 luni la 2 ani sau cu amendă;

(7) Acţiunea penală se pune în mişcare la plângerea prealabilă a persoanei vătămate;

(8) Prin imagine intimă se înțelege orice reproducere, indiferent de suport, a imaginii unei persoane nude, care își expune total sau partial organele genitale, anusul sau zona pubică sau, în cazul femeilor, sânii, ori care este implicată într-un raport sexual sau act sexual;

(9) Nu constituie infracţiune fapta săvârşită:

(a) dacă a fost necesară pentru prevenirea, surprinderea sau dovedirea săvârșirii unei infracțiuni;

(b) dacă a fost autorizată, în cazuri temeinic justificate, de către un organ judiciar în cursul unor proceduri judiciare."[48]

2.3.3. Cazul Germaniei

Odată cu intrarea în vigoare a Convenției de la Lanzarote și a Convenției de la Budapesta, legislația penală germană a fost adaptată pentru a încorpora evoluțiile recente în domeniul internetului și al criminalității informatice. Ulterior, legislația germană a încorporat, de asemenea, directive importante ale UE privind atacurile informatice și protecția copiilor împotriva abuzului sexual și a exploatării minorilor și a pornografiei infantile. Modificări importante au fost definiția penală a îngrijirii minorilor și modificarea sancțiunilor în conformitate cu Convenția de la Lanzarote.

[48] Pentru mai multe informații despre legea propusă privind pornografia non-consensuală, consultați https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019.

BKA (Departamentul Penal al Poliției Federale) este **autoritatea publică** responsabilă de **criminalitatea informatică**, pe plan intern și în ceea ce privește cooperarea internațională, în special în domeniul fraudelor de carduri online. De asemenea, BKA lucrează direct în lupta împotriva criminalității informatice cu agenții precum Interpol și Europol.

Ministerul de Interne a dezvoltat strategii naționale de combatere a criminalității informatice, consolidarea securității în telecomunicații și sisteme informatice și îmbunătățirea protecției acordate utilizatorilor de internet din Germania. Prima strategie a intrat în vigoare în 2011 și obiectivele sale sunt încă în mare măsură aplicabile astăzi. Cu toate acestea, evoluția rapidă a fenomenului a făcut necesară, în 2016, completarea acestor obiective și gruparea lor într-o nouă strategie care este transversală serviciilor pentru a promova și a accelera cooperarea între diferiți actori, ținând cont de încrucișarea -natura sectorială a criminalității informatice[49].

În ceea ce privește diplomele juridice privind lupta împotriva criminalității cibernetice, începând de la preceptul constituțional care prevede inviolabilitatea telecomunicațiilor, până la dispozițiile privind criminalitatea din Codul penal german și se încheie în legislație separată, cum ar fi **Legea telecomunicațiilor** (Telekommunikationsgesetz **TKG**), **Telemedia Act** (Telemediengesetz **TMG**), **Computer Security Act** (**IT-Sicherheitsgesetz**) și **Facebook Act** (Netzwerkdurchsetzungsgesetz **NetzDG**), sistemul juridic german pare să fie legal bine echipat pentru a combate realitatea dinamică și transfrontalieră a criminalității informatice, investind în cooperarea cu entități din industria privată.

Articolul 10 din Constituția Germaniei protejează inviolabilitatea secretului corespondenței poștale și a telecomunicațiilor.

În ceea ce privește dreptul penal, **Codul penal german** (Strafgesetzbuch **StGB**) reunește principalele infracțiuni legate de criminalitatea informatică și nu există nicio fragmentare între dreptul penal general și legea privind criminalitatea informatică, spre deosebire de sistemul juridic portughez.

StGB prevede trei tipuri de infracțiuni legate de criminalitatea informatică:

1. Conduite privind **utilizarea ilegală a sistemelor sau datelor computerizate**, în special legate de atacurile cibernetice:

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

Quadro I-5: Condutas respeitantes ao uso ilegítimo de sistemas ou dados informáticos

Articol si titlu	Conduită	Articol in CCCE
§ 202a – **Spionaj de date**	Obținerea accesului neautorizat la datele transmise electronic (sau a unui sistem de informații) care nu sunt destinate celor care le accesează sau a accesului neautorizat la date special protejate, ocolind mecanismele de securitate (de exemplu, criptarea).	2
§ 202b – **Interceptarea datelor computerizate (Phishing)**	Obțineți date la care accesul nu este autorizat utilizând o transmisie de date nepublică sau o radiație electromagnetică de la un sistem de procesare a datelor către sine sau către o altă persoană căreia nu este destinată comunicarea. Permite concursuri cu alte infracțiuni.	3
§ 202c – **Actele pregătitoare pentru spionaj și interceptarea ilegală a datelor computerizate (phishing)**	Practicarea actelor pregătitoare pentru infracțiunile prevăzute la § 202a și 202b; de exemplu. produce, obține pentru sine sau pentru alții, vinde, furnizează, dezvăluie sau face publice coduri de securitate care permit accesul sau programe de calculator al căror scop este practicarea unor astfel de acte.	6
§ 202d - **Manipularea ilegală a datelor computerului**	Obținerea, furnizarea, livrarea, distribuirea sau punerea la dispoziție a datelor care nu sunt în general accesibile sau deschise publicului și care au fost **obținute de o altă persoană printr-un act** ilicit, pentru a se îmbogăți pe sine sau pe alții sau pentru a dăuna altei persoane. Excepție: acte efectuate exclusiv în conformitate cu obligațiile legale, de ex. autoritatea publică în contextul unei anchete.	
§ 303a - **Manipularea datelor computerului**	Ștergerea, suprimarea, a face inutilizabile sau modificarea datelor computerului.	4
§ 303b – **Sabotajul computerului**	(1) Întreruperea în mod semnificativ a unei operațiuni de prelucrare a datelor care are o importanță esențială pentru o altă persoană prin efectuarea actelor descrise la § 303; sau prin introducerea sau transmiterea datelor cu intenția de a provoca un alt dezavantaj; sau prin distrugerea, deteriorarea, inutilizarea, eliminarea sau modificarea unui sistem de prelucrare a datelor sau a unui suport de date. (5) Se aplică articolului 202c, privind condamnarea actelor pregătitoare sau facilitatoare.	5
§ 269 – **Falsificarea datelor computerizate**	Pentru a induce în eroare relațiile juridice, pentru a stoca sau modifica dovezile relevante în așa fel încât să se producă un document fals sau falsificat sau pentru a utiliza datele stocate sau modificate în acest mod.	7
§ 270 – **Falsitate în prelucrarea datelor**	Înșelăciunea în raporturile juridice este echivalentă cu interferența în procesarea computerizată a datelor în raporturile juridice.	7

2. Conduite corespunzătoare unei **acțiuni a cărei practică necesită utilizarea mijloacelor electronice ca instrument** pentru comiterea infracțiunii:

Articol si titlu	Conduită	Articol in CCCE
§ 206 – **Încălcarea secretului poştal sau al telecomunicaţiilor**	(1) comunică altei persoane, fără autorizaţie, fapte care fac obiectul secretului poştal sau al telecomunicaţiilor şi despre care cineva a devenit conştient ca proprietar sau angajat al unei companii care furnizează servicii poştale sau de telecomunicaţii pe bază comercială. (5) Secretul traficului poştal se extinde la circumstanţele detaliate ale livrării şi la conţinutul acesteia. **Conţinutul telecomunicaţiilor şi circumstanţele sale specifice** (pentru cei implicaţi într-o operaţiune de telecomunicaţii) sunt **supuse secretului telecomunicaţiilor**. Secretul telecomunicaţiilor se extinde şi la circumstanţele **încercărilor de conectare nereuşite**.	
§ 263a – **Frauda computerizată**	(1) Cu intenţia de a obţine un avantaj patrimonial ilegal pentru sine sau pentru o terţă parte, de a deteriora proprietatea altei persoane prin influenţarea rezultatului unei operaţiuni de prelucrare a datelor prin proiectarea incorectă a programului, utilizarea de informaţii incorecte sau incomplete date, utilizarea neautorizată a datelor sau orice altă influenţă neautorizată asupra operaţiunii. (3) Actele pregătitoare, cum ar fi producţia, achiziţia, oferta de vânzare, întreţinerea în siguranţă sau livrarea către o altă persoană a programelor de computer al căror scop este practicarea unei astfel de infracţiuni.	8
§ 265a – **Obţinerea serviciilor prin înşelăciunemodo fraudulento**	Utilizarea unei maşini sau **reţele** de **telecomunicaţii** care serveşte scopurilor publice, pentru a nu plăti taxa datorată pentru un mijloc de transport sau accesul la un eveniment sau la o instalaţie.	

3. Conduite corespunzătoare unei **acțiuni care poate fi practicată** - dar nu neapărat - **prin utilizarea mijloacelor electronice** ca instrument pentru comiterea infracțiunii.

În acest caz, este important de menționat **articolul 11 alineatul (3)** care prevede că suporturile media precum **sunetul și imaginile, suporturile de stocare a datelor**, ilustrațiile și alte reprezentări trebuie să fie tratate în același mod în scopul articolelor care se referă la aceasta paragraf. Rezultă că următoarele infracțiuni implicate se comportă prin mijloace electronice:

Articol si titlu	Conduită
§ 86 – **Diseminarea materialului de propagandă al organizațiilor neconstituționale**	Utilizarea materialelor de propagandă - menționate la 11 (3) - care, conform conținutului lor, sunt îndreptate împotriva ordinii de bază democratice libere sau a principiilor dreptului internațional, sunt distribuite în Germania sau sunt produse, stocate, importate sau exportate pentru distribuire în Germania sau în străinătate, sau făcute accesibile publicului pe dispozitive de stocare a datelor.
§ 88 – **Sabotaj anticonstituțional**	(1) oricine acționează cu intenția de a interveni ... (2) facilități de telecomunicații de serviciu public.
§ 91 – **Incitare la comiterea unor infracțiuni violente grave împotriva statului**	Afișarea sau furnizarea unui alt material menționat la 11 (3) care, prin conținutul său, este capabil să servească ca instrucțiune de a comite infracțiuni grave și violente împotriva statului (§ 89a), în cazul în care circumstanțele diseminării sale sunt favorabile incitării sau încurajarea altor persoane să comită astfel de infracțiuni și / sau (2) Obținerea de materiale 11 (3) în scopul descris la (1) din acest articol.
§ 130 – **Incitare la ură**	(2) Incitare la ură, apel la măsuri violente sau atacarea demnității umane a unui grup sau a unor părți ale populației sau a unei persoane datorită apartenenței la un grup, prin mijloacele menționate la 11 (3), prin diseminarea materialelor public prin intermediul telecomunicațiilor. (5) Aprobarea publică, negarea sau minimizarea unui act de ură săvârșit în timpul domniei național-socialismului și perturbarea păcii publice într-o manieră care încalcă demnitatea victimelor prin aprobarea, glorificarea sau justificarea conduitei violenței regimului național socialist. și arbitrariul, se pedepsește la fel dacă sunt utilizate telecomunicațiile pentru comiterea sa.
§ 131 – **Descrieri ale violenței**	(1) Prin mijloacele menționate la 11 (3), descriere actelor de violență crudă sau inumană împotriva ființelor umane sau glorificarea sau banalizarea acestor acte prin diseminarea către public sau prin producție, achiziție, furnizare, stocare, ofertă, publicitate sau angajându-se să importe sau să exporte astfel de conținut, prin utilizarea mijloacelor de radiodifuziune și de telecomunicații.
§ 201a – **Încălcarea confidențialității intime prin realizarea de fotografii sau alte imagini**	(1) Crearea sau transmiterea / difuzarea înregistrării neautorizate a imaginii unei alte persoane în sfera sa intimă și privată. (3) Realizarea de fotografii, producerea sau furnizarea către o terță parte în schimbul unui beneficiu sau, obținerea pentru ei înșiși sau pentru o terță parte, a materialelor referitoare la goliciunea persoanelor sub 18 ani.
§ 238 – **Stalking**	Perturbarea severă a vieții altei persoane în așa fel încât să îi afecteze serios stilul de viață prin persistență: 1. căutarea apropierii fizice de acea persoană, 2. încercarea de a stabili contactul cu persoana respectivă prin utilizarea telecomunicațiilor, 3. utilizarea necorespunzătoare a date cu caracter personal în scopul (a) comandării de bunuri și servicii în numele acelei persoane, (b) inducerea unor terțe părți să ia contact cu persoana respectivă sau 4. amenințarea acelei persoane, a uneia dintre rudele lor sau a unei persoane apropiate, cu vătămări ale vieții, integrității fizice, sănătății sau libertății.

În ceea ce privește infracțiunile legate de minori, deși se încadrează în această din urmă categorie (3), acestea sunt tratate aici separat:

Articol si titlu	Conduită	Articol in CCCE
§ 176 – **Abuzul sexual asupra copiilor**	[1] Întreținerea de acte sexuale cu copii sub 14 ani; [2] Inducerea sau influențarea unui copil să efectueze acte de natură sexuală; [4] Angajarea în activități sexuale în prezența unui copil sau prezentarea acestuia de conținut pornografic prin mijloacele descrise la § 11 [3] sau prin tehnologiile informației și comunicării pentru a-l determina pe copil să se angajeze în activități sexuale cu infractorul sau o terță persoană, sau în prezența lor, sau pentru a influența copilul să se angajeze în acte pentru producerea de conținut de pornografie infantilă; [5] Oferirea sau promiterea de a furniza conținut copiilor cu privire la actele descrise de la [1] la [4].	9
§ 176a – **Abuzul sexual agravat al minorilor**	[3] Înfăptuirea faptelor descrise la § 176 ca infractor principal sau implicat în alt mod în săvârșirea faptelor, cu intenția de a face actul obiectul conținutului pornografic [§ 11 [3]] care să fie difuzat conform descrierii de la § 176b.	
§ 184b – **Diseminarea și achiziționarea de pornografie infantilă (sub 14 ani)**	Diseminarea, afișarea sau punerea în alt mod la dispoziția publicului a conținutului sexual al minorilor sau producerea, obținerea, furnizarea, stocarea, oferirea, recomandarea, importul sau exportul în aceste scopuri sau facilitarea / susținerea în alt mod a utilizării mijloacelor descrise în § 11 [3] referitoare la conținutul sexual al minorilor (include actele sexuale efectuate cu minori, actele efectuate în prezența minorilor sau reproducerea unui copil complet sau parțial dezbrăcat într-o poziție sexuală explicită sau reproducerea organelor genitale sau a feselor unui copil). [5] Exclude aplicarea în cazurile de exercitare legală a funcțiilor publice (de exemplu, în cadrul procedurilor penale).	
§ 184c – **Diseminarea, achiziționarea și deținerea de literatură pornografică pentru tineri**	Prin mijloacele descrise la § 11 [3], diseminarea sau punerea la dispoziția publicului, angajarea să livreze unei alte persoane sau să producă, să obțină, să furnizeze, să stocheze, să ofere, să facă publicitate sau să importe sau să exporte un tip de pornografie pentru tineri (între 14 - 18 ani).	
§ 184d – **Diseminarea conținutului pornografic prin radiodifuziune sau telecomunicații**	[1] Punerea la dispoziție a conținutului pornografic a altei persoane sau a publicului prin radio sau telecomunicații se pedepsește în conformitate cu prevederile §§ 184-184c (Nu se aplică cazurilor descrise în § 184 [1] - diseminarea conținutului pornografic - cu condiția ca un astfel de conținut se referă la persoane cu vârsta peste 18 ani și nu este accesibil persoanelor sub 18 ani]; [2] Acest lucru se aplică și pentru §§ 184b [3] și 184c [3]: oricine se obligă să procure conținut pornografic infantil prin mijloace electronice va fi, de asemenea, pedepsit.	

Încercarea se pedepsește în temeiul articolelor 263a (2) coroborat cu § 263 (2), § 269 (2), § 263a (3), § 303a, § 303b (vg. § 303a (2) și 303b (3)) . Pentru infracțiunile legate de abuzul asupra copiilor, tentativa este, de asemenea, pedepsită; § 176 (6). Excepție: § 176 (4) 3 și 4 și § 176 (5). Actele pregătitoare se pedepsesc în infracțiuni: § 202c, § 202a, § 202b, § 303a (1) (2) și § 303b (1) (5). Ajutorul și implicarea sunt, de asemenea, pedepsite în temeiul articolelor 26 și 27 din StGB.

Persoanele juridice nu sunt supuse răspunderii penale, dar pot fi făcute responsabile în conformitate cu §§ 30, 130 *Ordnungswidrigkeitengesetz* (OWiG), care se referă la Legea privind infracțiunile administrative. Reprezentanții lor legali pot fi trași la răspundere în conformitate cu articolul 14 din StGB.

Pe lângă infracțiunile descrise mai sus, legislația germană prevede și alte infracțiuni și contravenții în legătură cu acte referitoare la comunicații electronice și protecția datelor, pe care le descriem pe scurt.

Legea privind **telecomunicațiile (TKG)**, adoptată la 22.06.2004, prevede un set de obligații pentru furnizorii de servicii de telecomunicații, ca entități private, de respectat în exercitarea activității lor. Această lege are, de asemenea, o importanță deosebită în ceea ce privește problema conservării dovezilor digitale, deoarece prevede obligația de a raporta acte care pot constitui încălcări ale inviolabilității telecomunicațiilor și obligația de a păstra anumite date în scopuri de urmărire penală în cazul infracțiuni deosebit de grave.

Astfel, **§ 88 Confidențialitatea telecomunicațiilor** și **§ 89 Interzicerea interceptării, obligația operatorilor de echipamente destinate să păstreze confidențialitatea** protejează integritatea și confidențialitatea telecomunicațiilor și acoperă conținutul acestora și circumstanțele detaliate, de ex. cine este sau a fost implicat într-un proces de telecomunicații și, de asemenea, se extinde la detalii despre încercările nereușite de a stabili o conexiune. Este interzis părților să obțină cunoștințe despre aceste telecomunicații dincolo de ceea ce este strict indispensabil pentru exercitarea activității lor, iar utilizarea acestor cunoștințe în alte scopuri este permisă numai în măsura permisă de lege sau de alte dispoziții legale. În acest caz, este important de menționat că obligația de raportare prevăzută la § 138 din Codul penal - obligația de a raporta infracțiunile de care au cunoștință - are prioritate în raport cu secretul comunicărilor.

§90 interzice **utilizarea abuzivă a echipamentelor de transmisie** prin interzicerea deținerii, fabricării, distribuției, importului sau introducerii oricărui transmițător sau a altor echipamente de telecomunicații care sunt deosebit de potrivite și destinate să audă cuvântul nerostit al altei persoane sau să înregistreze imaginea altei persoane fără ca acea persoană să observe.

§96 și §98 se referă la condițiile în care furnizorii de servicii pot colecta date despre trafic și respectiv despre locație. Prin urmare, numai datele indispensabile în scopurile activității lor pot fi păstrate și aceste date pot fi utilizate numai în măsura necesară și în scopurile menționate în prezenta lege sau în conformitate cu alte dispoziții legale. În caz contrar, acestea trebuie șterse fără întârzieri nejustificate.

§109 obligă furnizorii de servicii să adopte **garanții tehnice** pentru a proteja secretul telecomunicațiilor și împotriva încălcării protecției datelor cu caracter personal, luând măsurile tehnice adecvate în prelucrarea datelor pentru a proteja utilizatorii împotriva perturbărilor cauzate de atacuri externe. Astfel, ar trebui luate măsuri pentru a proteja sistemele de telecomunicații și prelucrarea datelor de accesul neautorizat și pentru a minimiza efectele încălcărilor de securitate asupra utilizatorilor sau rețelelor interconectate. Punctul (5) din această secțiune prevede, de

asemenea, obligația de a raporta Agenției Federale de Rețea și Oficiului Federal pentru Securitatea Informațiilor orice deficiențe în rețelele și serviciile de telecomunicații care ar putea duce la încălcări semnificative ale securității. În mod similar, **§ 109a** privind **securitatea datelor și informațiilor** stabilește obligațiile de raportare în cazul unei încălcări a datelor cu caracter personal către Agenția Federală de Rețea și Comisarul Federal pentru Protecția Datelor și Libertatea de Informare a încălcării și către utilizatorii vizați.

În ceea ce privește păstrarea datelor în scopuri de probă digitală, **§ 113b** stabilește **obligația de a păstra datele de trafic** timp de 10 săptămâni pentru datele de trafic și timp de 4 săptămâni pentru datele de localizare. Conținutul este exclus. Furnizorul de servicii șterge datele stocate ireversibil fără întârziere, cel târziu în termen de o săptămână de la sfârșitul perioadelor de stocare prevăzute sau asigură ștergerea ireversibilă, de ex. dreptul de a fi uitat.

§ 113c stabilește **condițiile în care datele stocate pot fi utilizate** pe baza **articolului 113b**; acestea pot fi transmise unei autorități de urmărire penală numai dacă aceasta din urmă solicită o astfel de transmitere, se referă la o dispoziție legală care îi permite să colecteze astfel de date și dacă datele se referă la urmărirea penală a infracțiunilor penale deosebit de grave.

Ca măsură de securitate, **articolul 113d obligă furnizorii să asigure securitatea datelor stocate** pe baza obligației prevăzute la articolul 113b alineatul (1). Prin urmare, datele trebuie protejate împotriva accesului și utilizării neautorizate prin măsuri tehnice și organizaționale în conformitate cu stadiul tehnicii, prin utilizarea metodelor de criptare, printre altele.

Agenția Federală de Rețea are puterea de a **monitoriza aplicarea obligațiilor prevăzute** în prezenta lege pentru furnizorii de servicii **(§ 115)**. La rândul lor, aceștia sunt obligați să furnizeze informațiile necesare Agenției, care are puterea de a impune penalități cu titlu cominatoriu.

Legea Telemedia (Telemediengesetz **TMG**), adoptată la 26.02.2007, se aplică tuturor serviciilor de informații și comunicații electronice, cu excepția cazului în care acestea sunt servicii de telecomunicații. Rețineți obligația furnizorilor de servicii de informații și pagini web sau servicii de aplicații sau pentru smartphone-uri de a se asigura, prin acorduri adecvate și proporționale din punct de vedere economic, că accesul neautorizat nu este posibil **(§ 13 (7)**). Pe de altă parte, există și **datoria de a furniza informații în caz de acces ilegal la date (§ 15a)**.

Legea privind securitatea IT *(IT-Sicherheitsgesetz)*, adoptată la 25 iulie 2015, conferă jurisdicția parchetului federal pentru investigarea și urmărirea penală a infracțiunilor prevăzute la 202a, 202b, 202c, 263a, 303a și 303b din Codul penal.

Acesta își propune să consolideze securitatea sistemelor informatice și IT și face parte din strategia de securitate informatică aprobată în 2011. În acest scop, prevede obligații privind un nivel minim de securitate a computerelor pentru companiile de telecomunicații, furnizorii de servicii digitale și

operatorii de infrastructură critică, de ex. necesită implementarea unui sistem de gestionare a securității IT, prevede obligații de raportare către Departamentul Federal pentru Securitate Informatică (BSI) și către consumatori în caz de încălcare a sistemului IT și necesită colectarea informațiilor necesare pentru evaluarea riscurilor în securitatea tehnologia informației, sub formă de rapoarte privind atacurile care au avut loc, proceduri adoptate și riscuri iminente, care urmează să fie raportate autorităților federale (§ 4).

O propunere de modificare a acestei legi, Legea securității IT (IT-Sicherheitsgesetz) 2.0, era în așteptare la momentul redactării[50]. Noua propunere se bazează pe o schimbare de strategie în lupta împotriva criminalității informatice, care nu ar trebui să mai fie defensivă, ci ofensivă, prin utilizarea diferitelor tactici IT[51]. Propunerea prevede, de asemenea, sancțiuni sporite în temeiul Codului penal pentru infracțiuni informatice în conformitate cu secțiunile 202a, 202b, 202c, 202d, 303a și 303b StGB. În plus, §§ 202e și 202f sunt inserate după § 202d StGB:

- § 200e - Utilizarea neautorizată a sistemelor de tehnologie a informației;
- § 202f - Infracțiuni deosebit de grave împotriva secretului și integrității sistemelor TIC.

***Netzwerkdurchsetzungsgesetz* (NetzDG)**, publicat la 01.09.2017, cunoscut în mod obișnuit sub denumirea de Facebook Act, stabilește obligații și stabilește amenzi pentru furnizorii de rețele sociale în legătură cu gestionarea plângerilor utilizatorilor cu privire la infracțiuni de ură și alte conținuturi ilegale pe internet, precum și ca obligație trimestrială de raportare a furnizorilor. De asemenea, conferă dreptul la despăgubire pentru încălcarea drepturilor personale și dreptul la informații cu privire la datele infractorului înregistrate pe platforma respectivă, înainte de o hotărâre judecătorească[52].

§1 (3) definește conținutul considerat ilegal[53], inclusiv discriminarea și incitarea la discursurile de ură și la extrema dreaptă. §2 definește obligația de a raporta periodic cu privire la gestionarea plângerilor privind conținutul ilegal pe platformele lor. Acest raport trebuie să fie public. Oficiul Federal al Justiției (BfJ) este autoritatea administrativă care monitorizează rapoartele, cf. § 4 (4).

§ 3 (2) 2 prevede **obligația de a elimina sau de a bloca accesul la conținut vădit ilegal în termen de 24 de ore** de la primirea plângerii, cu excepția cazului în care se convine altfel cu poliția sau autoritățile judiciare. Alt conținut ilegal trebuie eliminat sau blocat accesul fără întârziere, în termen de maximum șapte zile de la primirea reclamației, cf. § 3 (2) 3. În caz de eliminare, furnizorul este obligat să păstreze conținutul în scopuri de probă. Prin urmare, stochează un astfel de conținut pentru o perioadă de zece săptămâni în domeniul de aplicare al Directivelor 2000/31 /EC și 2010/13 /EU, cf. § 3 (3).

Nerespectarea acestor obligații va duce la sancțiuni administrative.

În ceea ce privește obligațiile procedurale, obligațiile speciale prevăzute la articolele 16 și 17 din Convenția privind criminalitatea informatică nu sunt prevăzute în mod specific în **Codul de procedură penală german** (StPO). Cu toate acestea, confiscarea datelor informatice, inclusiv cererile de divulgare a datelor, se efectuează în temeiul articolelor 94 și 98 StPO, care reglementează confiscarea generală a activelor corporale.

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

[51] 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/

[52] Furnizorii de servicii de rețele sociale cu mai puțin de două milioane de utilizatori înregistrați în Germania sunt în afara domeniului de aplicare al prezentului regulament.

[53] Acestea sunt Articolele 86, 86a, 89a, 91, 100a, 111, 126, 129, 129a 129b, 130, 131, 140, 166, 184b, coroborate cu Articolele 184d, 185 la 187, 201a, 241 sau 269 din Codul Penal.

Articolul 18 al Convenției privind criminalitatea informatică nu este prevăzut ca atare în StPO. În acest sens, solicitarea de către autorități de divulgare / informații cu privire la datele informatice este acoperită de dispozițiile articolului 95 StPO, referitoare la obligația de a preda bunuri corporale relevante pentru probe în cadrul procedurilor penale.

Colectarea datelor privind traficul de comunicații în timp real, prevăzută la art. 20 din Convenția privind criminalitatea informatică, este supusă cerințelor din § 100g StPO. Acest articol precizează, de asemenea, care infracțiuni deosebit de grave justifică furnizarea de date de către furnizorii de servicii (cf. § 113b TKG). § 100g (2) prevede, de asemenea, posibilitatea instanței de a dispune furnizarea de date și informații despre trafic către furnizorii de servicii în caz de suspiciuni întemeiate cu privire la infracțiunea deosebit de gravă enumerată în articolul respectiv.

Interceptarea telecomunicațiilor sau colectarea datelor în timp real prevăzute la art. 21 din Convenția privind criminalitatea informatică este reglementată de articolele 100a și 100b. Acesta trebuie să facă obiectul autorizării judiciare la cererea procurorului. În general, colectarea datelor prin căutare online și spyware nu este admisă în domeniul urmăririi penale, cu excepția cazurilor descrise la 100b.

§ 110 (3) - Posibilitatea accesului și inspecției mediilor de stocare separate spațial de cea principală care se afla sub inspecție, în măsura în care acestea pot fi accesate din mediul de stocare. Exemplu: discuri externe.

Cererile de informații și / sau livrarea de date de la furnizorii de servicii către autorități sunt reglementate în general în § 100j StPO și în special în legi separate; de exemplu. § 113 TKG.

Informațiile și datele sunt furnizate în limitele prevăzute la § 96 (1), § 113a și 113b TKG (Legea telecomunicațiilor).

În ceea ce privește **cooperarea internațională**, Germania este implicată în mai multe proiecte europene și internaționale de cooperare bilaterală în domeniul securității informatice:

- Agenția Europeană pentru Securitatea Rețelelor și Informațiilor (ENISA);
- Programul AGIS al Comisiei Europene, conceput pentru a ajuta practicienii juridici, precum și autoritățile judiciare și reprezentanții serviciilor de asistență pentru victime din statele membre și din alte țări care aplică, în vederea înființării unei rețele europene de schimb de informații și bune practici;
- Grupul de lucru european Interpol privind criminalitatea IT (EWPITC), o platformă pentru schimbul de informații și combaterea criminalității IT.

Legea internațională privind asistența, în germană **Internationale Rechtshilfe in Strafsachen (IRG)**, prevede proceduri și condiții pentru asistența internațională. Astfel, articolele 29-31 din Convenția privind criminalitatea informatică privind asistența reciprocă între țări sunt reglementate de această lege.

În ceea ce privește cooperarea cu Centrul Europol pentru combaterea criminalității informatice, Germania face parte din grupul de lucru comun pentru acțiunea împotriva criminalității informatice (J-CAT)[54].

[54] https://www.europol.europa.eu/content/expert-international-cyber-crime-taskforce-launched-tack-le-online-crime Participanți: Austria, Canada, Germania, Franța, Italia, Olanda, Spania, Marea Britanie și SUA. Australia și Columbia s-au angajat la inițiativă.

Punctul de contact 24/7 în conformitate cu articolul 35 din Convenția de la Budapesta este stabilit la BKA din Wiesbaden împreună cu punctul de contact Interpol și G-8.

Mai mult, există unele **parteneriate public-private** în Germania pentru a **combate criminalitatea informatică**, în special;

- Alianța pentru securitatea informatică: promovează schimbul de informații și experiențe între jucătorii cheie din arena germană de securitate informatică și își propune să acționeze ca o platformă de informare despre riscurile predominante în spațiul informatic și să promoveze schimbul de cunoștințe. O inițiativă comună a Oficiului Federal German pentru Securitatea Informației (BSI) și a Asociației Federale Germane pentru Tehnologia Informației (Bitkom);
- Rețea CERT - Rețeaua CERT este alianța echipelor IT de intervenție în caz de urgență[55].

Note finale

- Simpla deținere de programe malware nu este incriminatoare. Legislația națională incriminează aceste fapte doar atunci când o persoană le folosește în mod penal.
- Potrivit unor profesioniști, dispozițiile legale trebuie introduse în Codul de procedură penală pentru a include utilizarea instrumentelor de acces la date, cum ar fi hacking-ul, având în vedere că forțele de securitate consideră că sunt cu un pas în spatele infractorilor.
- În general, dreptul german pare să fie în conformitate cu textele legale europene.
- Cu toate acestea, nu există o transpunere expresă a articolelor 4 și 5 din Directiva 2019/713 / UE, întrucât trebuie să se utilizeze încă două infracțiuni generale (§§ 263a și 269 din Codul penal, respectiv frauda computerizată și falsitatea computerizată) infracțiuni legate de utilizarea frauduloasă a instrumentelor de plată fără numerar. § 152b din Codul penal prevede infracțiunea de falsificare a cardurilor de plată, dar nu face nicio referire la utilizarea mijloacelor electronice sau prin intermediul sistemelor IT.

[55] ttps://www.cert-verbund.de/

3. PERSPECTIVE CRIMINOLOGICE ȘI VICTIMOLOGICE PENTRU ÎNȚELEGEREA CRIMINALITĂȚII INFORMATICE

3.1. Teorii criminologice aplicate criminalității informatice

În acest capitol al Manualului, vom aborda pe scurt diferitele teorii ale criminalității și aplicarea lor la criminalitatea informatică, cu scopul de a realiza o lectură cât mai cuprinzătoare a fenomenului criminalității informatice.

Baza unei astfel de analize este premisa că cunoștințele existente despre criminalitatea tradițională sunt aplicabile și criminalității informatice, presupunând, prin urmare, că infracțiunile tradiționale și criminalitatea informatică nu sunt substanțial diferite. În acest sens, teoriile criminologice asociate cu criminalitatea tradițională devin instrumente valoroase pentru a explica și criminalitatea cibernetică (Wall, 2005, Yar, 2005b cit în Bossler & Burruss, 2012).

Cu toate acestea, este important să subliniem faptul că nu este posibil să se înțeleagă pe deplin fenomenul criminal și, în special, criminalitatea informatică, prin obiectivul exclusiv al unei singure teorii sau abordări criminologice și, prin urmare, este foarte important, chiar având în vedere complexitatea fenomenului analizat, pentru a lua în considerare împletirea acestor perspective (și a altor) în căutarea unei înțelegeri mai robuste a criminalității informatice și a victimizării informatice (Yar & Steinmetz, 2019).

3.1.1. Perspective individuale

Această abordare sugerează că persoanele cu un auto-control scăzut sunt mai predispuse să se angajeze în acte ilicite (Gottredson & Hirschi, 1990 cit în Maimon & Louderback, 2019).

În această privință, Gottfredson și Hirschi (1990 cit în Higgins, Ricketts & Wolfe, 2014) au susținut că persoanele cu **auto-control scăzut** sunt mai puțin capabile să reziste tentației atunci când se confruntă cu o oportunitate ilicită, minimizând consecințele acțiunilor lor, datorită caracteristicilor asociate cu această trăsătură individuală, și anume impulsivitatea și insensibilitatea (Gottfredson și Hirschi, 1990 cit in idem). În acest sens, criminalitatea este atractivă, deoarece oferă beneficii imediate, fără a lua în considerare sau anticipa impactul pe termen lung, atât la nivel individual, cât și pentru alții.

Aplicând această abordare explicativă a criminalității tradiționale la înțelegerea criminalității informatice, asocierea dintre caracteristicile individuale ale autorului criminalității informatice și criminalitatea informatică nu pare a fi atât de liniară, întrucât cercetările nu arată în mod unanim că nivelurile scăzute de autocontrol reprezintă (sau nu) un factor de risc individual pentru practicarea criminalității informatice (Maimon & Louderback, 2019).

În cazul criminalității informatice, caracteristicile individuale pot să nu fie atât de semnificative, deoarece criminalitatea informatică implică o interacțiune directă minimă (sau chiar inexistentă) între victimă și infractor. De exemplu, în cazul programelor malware, este dificil să se determine cine va fi victima efectivă a infecției cu software-ul rău intenționat, deoarece orice computer poate fi infectat, indiferent de caracteristicile individuale ale jucătorilor (Ngo & Paternoster, 2011).

Pe de altă parte, nivelurile de auto-control par să aibă impact asupra riscului de victimizare. Schreck, Stewart și Fisher (2006 cit în McNeeley, 2015) au identificat o asociere între autocontrol scăzut și o înclinație mai mică pentru a evita comportamentul riscant (cum ar fi implicarea în activități delincvente și socializarea cu colegii devianți), chiar și după experiențe personale de victimizare. Această legătură între autocontrolul scăzut și victimizarea repetată a fost confirmată de Turanovic și Pratt (2014 cit în McNeeley, 2015): persoanele cu niveluri scăzute de autocontrol au fost mai puțin susceptibile să facă schimbări în stilul lor de viață, chiar și după experiențe de victimizare.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Unele studii privind criminalitatea informatică, în special privind criminalitatea dependentă informatic, au **identificat factori de risc individuali asociați cu comiterea**:

- Există studii care afirmă că, în cazul infracțiunilor informatice, majoritatea autorilor au o **capacitate tehnică relativ scăzută** (NCA, 2016 cit în Maimon & Louderback, 2019).
- Alții indică, pe de altă parte, asocierea criminalității informatice cu **caracteristici psihologice și cognitive**, cum ar fi curiozitatea, gândirea creativă, capacitatea de rezolvare a problemelor și gândirea sistematică și tehnică (Rogers, 2006, Steinmetz, 2015 cit în Maimon & Louderback, 2019).

Alți autori (Morris, 2011 cit în Maimon & Louderback, 2019) atrag atenția asupra faptului că făptuitorul criminalității informatice, în special în cazul infracțiunilor dependente informatic, dezvoltă **atribuții cauzale clar externe**, precum tehnici de neutralizare și raționalizare, negând existența victimei, criminalitatea cibernetică și / sau responsabilitatea în faptă și / sau învinuirea victimei pentru faptul că practicarea criminalității informatice a fost posibilă.

În cazul hacking-ului, Van der Hulst și Snow (cit în Koops, 2010) au făcut distincție între 3 tipuri de hackeri, asociați cu motivații diferite:

- tineri infractori de sex masculin a căror practică a infracționalității informatice este asociată cu distracție, curiozitate sau respect pentru colegi;
- hackerii ideologici, care sunt inteligenți și dornici să învețe, dintre care unii sunt obsesivi și antisociali;
- hackeri motivați financiar.

3.1.2. Criminalitatea informatică ca alegere rațională

Cu o abordare opusă celei anterioare, în cadrul criminologiei neoclasice, infracționalitatea apare ca rezultat al proceselor cognitive raționale de reflecție și decizie ale autorilor respectivi. Aceasta înseamnă că infracțiunea corespunde unei decizii raționale din partea agentului său, care analizează costurile și beneficiile asociate practicii sale și ale cărui alegeri / decizii sunt ghidate de aceleași procese de analiză și reflecție (Cornish & Clarke, 1986 cit in Yar & Steinmetz, 2019).

Urmând această abordare, dacă potențialul contravenient percepe costurile asociate săvârșirii unei

infracțiuni, care pot include probabilitatea / riscul de a fi prins și consecințele juridice asociate, la fel de scăzute, în comparație cu câștigurile sau beneficiile obținute în cele din urmă în cazul unei astfel de infracțiuni, săvârșirea infracțiunii, probabilitatea apariției infracțiunii crește (Nagin, 1998 cit in idem).

Pe baza acestei interpretări, creșterea **costurilor percepute asociate săvârșirii unei infracțiuni** și / sau reducerea percepției **beneficiilor, câștigurilor și / sau recompenselor din comiterea acesteia** poate contribui la atenuarea infracțiunii (Cornish & Clarke, 1986 cit in idem).

Studii precum Louderback & Antonaccio (2017) indică faptul că procesele cognitive reflexive pot reduce sau crește riscul implicării în criminalitatea cibernetică. Această rațiune se bazează tocmai pe faptul că **criminalitatea informatică este înțeleasă ca o alegere**, în care se efectuează o evaluare rațională a eforturilor, costurilor și recompenselor asociate cu un anumit comportament (Cornish, 1993 cit în Maia și colab., 2016).

Unele studii asociate cu aplicarea acestei abordări în explicarea criminalității informatice (de exemplu, Bachmann, 2008, Hutchings, 2013 cit în Yar & Steinmetz, 2019) indică faptul că autorul criminalității informatice face efectiv alegeri raționale în alegerea țintelor lor și, de asemenea, în adoptarea comportamentelor de risc.

Alegerea rațională pare, de asemenea, să aibă loc chiar și atunci când țintele arată indicii clare de a putea declanșa consecințe asociate cu practicarea criminalității informatice, care există acolo ca elemente de descurajare. Acest lucru duce la o modificare a comportamentului infracțional, dar nu neapărat la descurajarea acestuia (de exemplu, Maimon și colab., 2013 cit in idem).

3.1.3. Teoria stilului de viață

Teoria **expunerii stilului de viață** dezvoltată de Hindelang, Gottfredson și Garofalo (1978 cit în Phillips, 2015) afirmă că stilul de viață zilnic al unei persoane influențează cantitatea de expunere la locurile și momentele în care există un risc mai mare de infracțiune.

În acest sens, diferențele în ratele de victimizare între diferite grupuri demografice se datorează tocmai variațiilor stilului de viață, care includ activități zilnice de rutină, activități profesionale (inclusiv ocupații profesionale și școlare / academice) și activități de agrement (Hindelang și colab., 1978, p 241 cit în McNeeley, 2015) și care poate crește sau reduce expunerea la locuri și persoane cu risc ridicat în momentele în care este cel mai probabil să se producă infracțiuni.

Aceeași teorie postulează că caracteristicile demografice, cum ar fi vârsta, sexul, starea civilă, starea socioeconomică, educația și ocupația, afectează stilurile de viață, deoarece acestea au ca rezultat implicații pentru rolurile, comportamentele, activitățile și atributele construite social pe care o societate dată le consideră adecvate pentru o persoană cu anumite caracteristici.

În mod similar, **stilul de viață pe Internet** al unei anumite persoane, care include activități sociale, cum ar fi chat, publicarea și / sau partajarea de conținut pe rețelele sociale, activități profesionale, cum ar fi comunicarea prin e-mail, efectuarea de apeluri audio / video și / sau partajarea și stocarea fișierelor pe stocare și serviciile / aplicațiile de sincronizare, precum și activitățile de rutină, cum ar fi cumpărarea produselor, efectuarea plăților, consultarea site-urilor web și utilizarea aplicațiilor, pot fi văzute ca un factor determinant al expunerii la criminalitatea informatică (Van Wilsem, 2011).

Mai mult, stilul de viață al unei persoane influențează, de asemenea, riscul de a se angaja în activități ilicite, oferind posibilitatea de a se implica într-un comportament criminal (poate cu colegii devianți) și ținându-le departe de supravegherea colegilor și de alte relații de protecție (McNeeley, 2015).

Această teorie a fost combinată cu teoria activității de rutină, descrisă mai jos, pentru o explicație mai generală a criminalității / victimizării (idem).

3.1.4. Teoria Activititătii de Rutină

Pornind de la teoria stilului de viață, **teoria activităților de rutină** încearcă să explice apariția infracțiunilor prin combinarea următoarelor condiții:

- infractori motivați;
- țintă / victimă adecvată;
- absența tutelei (Cohen & Felson, 1979 cit în Maimon & Louderback, 2019).

Dacă una (sau mai multe) dintre aceste trei condiții este absentă, probabilitatea infracțiunii scade (Phillips, 2015).

În ceea ce privește **infractorii informatici**, apropierea victimei de infractorii informatici motivați crește riscul victimizării (Van Wilsen, 2013 cit în Maimon & Louderback, 2019).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Motivația pentru practicarea unei infracțiuni informatice poate fi **situațională**, și anume prin prezența unor stimuli care, indiferent de trăsăturile de personalitate, pot duce la implicarea în infracțiuni informatice (Briar & Piliavin, 1965 cit în Maimon & Louderback, 2019). Acești stimuli pot fi asociați cu apariția **infracțiunilor motivate de oportunitate** care, în cazul infracțiunilor dependente informatic, pot include vulnerabilități într-un sistem de operare dat, absența sistemelor de supraveghere și / sau disponibilitatea datelor necriptate. Aceste circumstanțe reduc riscul de detectare a infractorilor online, ceea ce la rândul său crește probabilitatea apariției criminalității informatice (Willison & Siponen, 2009 cit în Maimon & Louderback, 2019).

Adecvarea țintei / victimei este evaluată rațional de către infractor, prin valoarea sau dezirabilitatea țintei, vizibilitatea, inerția și accesibilitatea acesteia (Felson, 2002 cit în Maia și colab., 2016).

De asemenea, în ceea ce privește adecvarea țintei, în cazul criminalității informatice, având în vedere accesibilitatea și numărul de utilizatori de pe și ai internetului, oportunitățile pentru criminalitatea informatică sunt considerate a fi mai mari decât practica criminalității în lumea fizică (Saridakis , Benson, Ezingeard și Tennakoon, 2016).

Nivelurile de utilizare a TIC și a Internetului par a fi un indicator important al **adecvării țintelor**, adică persoanele cu perioade mai lungi de utilizare a TIC prezintă un risc mai mare de victimizare cibernetică. Studiul realizat de Wang și colegii (2015 cit în Maimon & Louderback, 2019) a arătat că, de fapt, accesibilitatea, vizibilitatea și expunerea unei ținte pot crește riscul victimizării informatice. Încă în sfera **adecvării,** criminalitatea informatică este, de asemenea, mai frecventă în țările mai bogate și, ca atare, cu mai mulți utilizatori de Internet (Kigerl, 2012 cit în Maimon & Louderback, 2019).

În ceea ce privește criminalitatea informatică îndreptată către companii și organizații, adecvarea țintei crește riscul de criminalitate informatică. În acest sens, criminalitatea informatică este mai frecventă în timpul orelor de lucru ale companiilor sau organizațiilor țintă, timp în care numărul potențialelor victime disponibile este mai mare (Kigerl, 2012 cit în Maimon & Louderback, 2019).

La rândul său, **tutela** în cazul criminalității informatice și, în special, a infracțiunilor dependente informatic, implică (Grabosky, 2016 cit în Maimon & Louderback, 2019):

- Autoritățile de poliție;
- Organizațiile guvernamentale responsabile de gestionarea și monitorizarea spațiului informatic;
- Furnizori de servicii Internet, companii și industrii care utilizează diferite instrumente și practici pentru a preveni criminalitatea informatică.

În ceea ce privește criminalitatea informatică, tutela poate fi analizată din diferite dimensiuni (Bossler & Holt, 2009, Holt & Bossler, 2013 cit în Maimon & Louderback, 2019). Prin urmare:

- absența **tutelei sociale** (de exemplu supravegherea părinților atunci când copiii folosesc internetul) pare a fi asociată cu o probabilitate crescută de criminalitate informatică;
- deși nu este acceptată în unanimitate, **tutela fizică** (care include utilizarea sistemelor de securitate TIC sau a software-ului) este asociată cu reducerea riscului de victimizare informatică;
- prezența **tutelei personale** (care privește cunoștințele și abilitățile de utilizare a TIC și a internetului) reduce criminalitatea informatică.

În concluzie, teoria stilului de viață și a activităților de rutină subliniază ideea că activitățile și comportamentele de rutină ale unei persoane își pot crește nivelul de adecvare ca țintă (potențială) a criminalității informatice și expunerea lor la infractori, care, în absența mecanismelor de tutelă, crește

riscul de victimizare și victimizare informatică (Cohen, Kluegel & Land, 1981 cit în Phillips, 2015).

3.1.5. Alte abordări relevante

Pe scurt, **teoria învățării sociale** înțelege criminalitatea ca un comportament învățat, ca orice alt comportament.

Acest proces de învățare implică:

- interacțiunile unui individ cu alții dintr-un anumit grup;
- atitudinile unui individ față de comportament, inclusiv tehnici, raționalizare și motivație pentru a efectua un comportament;
- imitație, inclusiv observarea și repetarea unui anumit comportament afișat de alte elemente ale grupului;
- întărire, inclusiv recompense care promovează inițierea și menținerea comportamentului.

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

Teoria învățării sociale pare, de asemenea, o explicație adecvată pentru criminalitatea informatică, întrucât înțelege comportamentul infracțional ca fiind învățat, printr-un proces de imitare de la egal la egal și asimilat prin mecanisme de întărire pozitivă, iar **asocierea cu semeni similari** pare să fie legată de implicarea în practica criminalității informatice (Hutchings & Clayton, 2016 cit în Maimon & Louderback, 2019).

În acest fel, se poate observa o progresie de la abordări sau perspective individuale, asociate cu caracteristicile psihologice, emoționale și procesele cognitive ale unui individ dat, până la relațiile lor interpersonale, unde este, de asemenea, important să se evidențieze **implicarea în rețele mai mult sau mai puțin organizate a colegilor din deep web**, cu propria **subcultură și structură (ierarhică)**, ca factor de risc pentru săvârșirea infracțiunilor informatice (Macdonald & Frank, 2017 cit in idem). De asemenea, trebuie spus că menținerea **loialității în relații** este subliniată în unele studii ca o motivație pentru implicarea în infracționalitatea informatică, în special în cazul infracțiunilor dependente informatic (Hutchings & Clayton, 2016 cit in idem).

Criminalitatea informatică poate fi explicată și în funcție de trei dimensiuni (Thornberry, Krohn, Lizotte & Chard-Wierschem, 1993 cit în Peterson & Densley, 2017):

- **selecție**: cauza criminalității informatice nu este Internetul în sine, ci mai degrabă factorii de risc individuali și înclinația criminală prezenți la persoanele care utilizează internetul, TIC și rețelele sociale;
- **facilitare**: Internetul și TIC au un efect asupra facilitării criminalității informatice, datorită unora dintre caracteristicile favorabile ale contextului online, cum ar fi anonimatul, lipsa / absența tutelei și procesele de grup (cum ar fi conformitatea cu normele de grup);
- **îmbunătățire**: care combină efectele enumerate mai sus - selecție și facilitare - explicând

faptul că apariția criminalității informatice este asociată cu **prezența factorilor de risc individuali la persoanele cele mai predispuse la practicarea criminalității informatice** și a **caracteristicilor menționate anterior ale internetului**, rețelelor sociale și TIC care sporesc expresia înclinației criminale.

3.2. Victima criminalității informatice și factorii de risc asociați cu victimizarea informatică

După cum s-a discutat deja în secțiunea 1 a acestui manual, „ecosistemul" criminalității informatice și diferitele sale forme de exprimare includ o parte adesea secundară sau neglijată în înțelegerea fenomenului infracțional: ne referim în mod specific la **victimele infracțiunilor**.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

În conformitate cu Directiva 2012/29 /EU a Parlamentului European și a Consiliului din 25 octombrie 2012 de stabilire a standardelor minime privind drepturile, sprijinul și protecția victimelor infracțiunilor[56], victima este definită ca:

i. *o persoană fizică care a suferit vătămări, inclusiv vătămări fizice, psihice sau emoționale sau pierderi economice cauzate direct de o infracțiune;*
ii. *membrii de familie ai unei persoane a cărei moarte a fost cauzată direct de o infracțiune și care a suferit un prejudiciu ca urmare a morții acelei persoane*

Cu alte cuvinte, **victima unei infracțiuni** este o persoană care, ca urmare a unei fapte comise prin încălcarea legilor penale în vigoare, a suferit un atac asupra vieții, integrității fizice sau mentale, suferinței emoționale sau pierderii materiale. Victimele sunt, de asemenea, considerate a fi rude apropiate sau dependente ale victimei directe, precum și persoane care au suferit un fel de rău atunci când au intervenit pentru a asista victimele sau pentru a preveni victimizarea.

Conform *Raportului IVOR: Implementarea reformei orientate către victime a sistemului de justiție penală în Uniunea Europeană*[57], un raport care reflectă asupra cercetării, cunoștințelor științifice și empirice privind punerea în practică a drepturilor victimelor infracțiunilor în Europa, o definiție clară, cel puțin din punct de vedere juridic, a conceptului de victimă a unei infracțiuni nu numai că contribuie la o mai bună susținere și protecție a victimelor, dar promovează și o mai mare **conștientizare și recunoaștere a statutului victimei** în fenomenul infracțional și în sistemul de justiție.

În acest moment din manual, vom încerca să oferim vizibilitate victimelor care, ca urmare a uneia (sau mai multor) infracțiuni informatic dependente și / sau a oricărei infracțiuni permise sau facilitate de internet și TIC, au suferit pierderi, fizic, moral, mental, emoțional sau material. Vom începe prin a aborda unii dintre factorii de risc asociați cu criminalitatea informatică.

[56] Documentul complet este disponibil la: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32012L0029&from=PT

[57] Informații suplimentare privind reflecția în jurul definiției conceptului de victimă a infracțiunilor și a altor aspecte legate de drepturile lor și punerea sa efectivă în aplicare sunt disponibile în raportul complet la https://apav.pt/publiproj/images/yootheme/PDF/IVOR-Repot-WebVersion.pdf .

3. PERSPECTIVE CRIMINOLOGICE ȘI VICTIMOLOGICE PENTRU ÎNȚELEGEREA CRIMINALITĂȚII INFORMATICE

Factorii de risc[58] se referă la caracteristicile, condițiile sau variabilele asociate cu o anumită persoană care cresc probabilitatea unor rezultate negative sau nedorite (Reppold și colab., 2002 cit în Maia și colab., 2016).

Ei pot fi statici sau dinamici. Caracteristicile statice sau condițiile persoanei și / sau ale trecutului acestora nu sunt schimbătoare, cum ar fi sexul, experiențele personale de violență din copilărie sau pierderea unei rude. Pe de altă parte, factorii de risc dinamici se referă la caracteristici, condiții sau variabile care pot fi modificate și cresc probabilitatea apariției unei anumite probleme.

Astfel, prin conceptualizarea criminalității cibernetice ca o problemă sau rezultat negativ, **factorii de risc** asociați cu victimizarea informatică sunt caracteristici sau condiții care pot crește probabilitatea sau vulnerabilitatea unei persoane la criminalitatea informatică.

Cercetările nu sunt deosebit de extinse în acest domeniu, ca în multe altele asociate cu înțelegerea criminalității informatice. Cu toate acestea, sunt evidențiate următoarele studii.

3.2.1. Factorii de risc asociați cu caracteristicile socio-demografice

Asocierea dintre **gen** și riscul victimizării cibernetice nu este directă și este important să se ia în considerare cel puțin diferitele tipuri de criminalitate informatică, altfel înțelegerea vulnerabilității la criminalitatea informatică va fi diminuată. Să examinăm câteva dintre informațiile disponibile.

Deși nu există consens, unele studii indică faptul că femeile sunt mai susceptibile de a fi victime ale criminalității informatic dependente (Bossler & Holt, 2009, 2010, Ngo & Paternoster, 2011 cit în Maimon & Louderback, 2019). Același lucru pare să fie valabil și pentru *cyberstalking* (Holt & Bossler, 2008), cu rate de prevalență mai mari care afectează femeile, precum și pentru bullying informatic.

Pe de altă parte, în cazul abuzurilor și exploatării sexuale online a copiilor, deși proporția fetelor victime este mai mare decât pentru copiii băieți, cel puțin în cazurile identificate, aceștia din urmă sunt de obicei ținta unor forme mai grave, severe și intruzive de agresiune sexuală[59].

În ceea ce privește expunerea (și anume a copiilor și tinerilor), de exemplu, la conținutul discursurilor de ură online, diferențele în media europeană a ratelor de expunere între copii / fete adolescente și copii / băieți adolescenți sunt minime. Același scenariu a fost identificat la recepția de conținut sexual / sexting auto-produs, cu medii foarte similare pentru ambele sexe[60].

La fel, **vârsta** relevă, de asemenea, în studiile și cercetările efectuate până în prezent, o relație inconsistentă cu riscul de victimizare informatică (Bossler & Holt, 2009, Ngo & Paternoster, 2011 cit în Maimon & Louderback, 2019). Cu toate acestea, unele studii indică faptul că persoanele în vârstă

[58] Pentru claritate, este important de reținut că conceptul de factor de risc nu poate fi disociat de conceptul de factor de protecție, care se referă la caracteristici sau condiții care pot diminua probabilitatea apariției sau apariției unei anumite probleme.

[59] Informații suplimentare detaliate sunt disponibile la adresa https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database .

[60] Vedeți rezultatele EU Kids Online 2020: rezultatele sondajului din 19 țări la https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf .

sunt, mai des decât alți adulții, victime ale infracțiunilor informatic dependente, cum ar fi hacking-ul (Leukfeldt & Yar, 2016 cit în Maimon & Louderback, 2019).

Pe de altă parte, și în termeni generali, populația mai tânără, așa cum vom aborda mai jos, are rate ridicate de utilizare intensivă a TIC și a Internetului, în special utilizarea rețelelor sociale, ceea ce va duce la o vulnerabilitate mai mare la victimizarea informatică în comparație cu utilizatori mai în vârstă și mai puțin frecvenți (Staksrud, ÓLafsson & Livingstone, 2013 cit în Näsi, Oksanen, Keipi & Räsänen, 2015; Näsi și colab., 2015).

În ceea ce privește **educația**, există studii care indică o posibilă relație negativă între nivelul de educație și victimizarea informatică, și anume pentru hacking, adică nivelurile superioare de educație vor fi asociate cu un risc mai mic de victimizare informatică (van Wilsem, 2013 cit în Maimon & Louderback, 2019). Cu toate acestea, la fel ca în caracteristicile socio-demografice anterioare, efectul acestui factor de risc necesită investigații suplimentare, având în vedere cunoștințele încă recente cu privire la riscul de victimizarea informatică asociat cu caracteristicile individuale.

3.2.2. Factorii de risc asociați cu utilizarea internetului și a TIC

Conceptul de **alfabetizare tehnologică** se referă la conștientizarea, cunoștințele și abilitățile care permit unei persoane să utilizeze Internetul, TIC și echipamentele și instrumentele asociate în mod eficient și să navigheze în mediile digitale (Holt & Bossler, 2013 cit în Maimon & Louderback, 2019).

Prin urmare, este un factor important în determinarea nivelurilor de risc și de protecție împotriva victimizării informatice. Abilitățile și cunoștințele legate de Internet și TIC par să reducă riscul de victimizare informatică, de asemenea, oferind utilizatorului o capacitate mai mare de a identifica și acționa în situații în care securitatea lor online poate fi expusă riscului (Holt & Bossler, 2008).

Există mai multe studii care indică existența unei creșteri a vulnerabilității la victimizarea informatică în diferite forme de criminalitate informatică, cum ar fi hacking, malware și phishing, în funcție de **nivelurile de utilizare a internetului și a TIC** (Yucedal, 2010; Leukfeldt & Yar, 2016 ; Reyens, 2015 cit în Maimon & Louderback, 2019). Se pare că există o asociere între nivelul de activitate în TIC și victimizarea informatice: persoanele cu utilizare sporită a rețelelor sociale și TIC în general în activitățile lor zilnice au, de asemenea, niveluri mai ridicate de experiențe personale de victimizare informatică (Butler, 2013). Această constatare este în concordanță cu teoriile criminologice deja discutate în acest manual.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Riscul crescut de victimizare informatică în funcție de nivelurile de utilizare a TIC nu ar trebui interpretat într-un mod liniar, unde utilizarea TIC și a internetului de la sine crește riscul de victimizare informatică.

În principal, **comportamentele și tipul de activități desfășurate atunci când se utilizează TIC și Internetul** sunt principalii factori care contribuie la vulnerabilitatea crescută la victimizarea informatică (Butler, 2013; Holt & Bossler, 2008).

Această vulnerabilitate va fi abordată mai detaliat în următoarea secțiune a acestui manual.

3.2.3. Vulnerabilitatea comportamentală și asocierea acesteia cu victimizarea informatică

IMPORTANT | STATISTICI IN FOCUS:

Conform datelor din studiul transnațional menționat anterior *Comportamentul sănătății la copiii de vârstă școlară*, 35% dintre elevii chestionați se consideră a fi **utilizatori foarte intensivi ai internetului și TIC**, adică utilizează aceste instrumente zilnic și pentru o parte semnificativă a zilei.

Mai mult, 1 din 10 elevi de școală raportează o utilizare intensivă a internetului și a TIC pentru a comunica cu oamenii pe care i-au întâlnit doar prin intermediul internetului.

În medie, aproximativ 7% dintre elevii școlii dezvăluie, de asemenea, **comportamente dependente** asociate cu utilizarea internetului și a TIC, în special pentru respondenții de sex feminin.

Așa cum s-a menționat în legătură cu teoria stilului de viață și teoria activității de rutină (a se vedea secțiunea 3.1. din acest manual), stilul de viață online al unei persoane își afectează riscul de victimizare informatică (Yucedal, 2010).

După cum se remarcă prin abordările teoretice ale criminologiei, stilul de viață online include **tot felul de activități desfășurate pe internet sau prin internet și TIC**, fie în ceea ce privește interacțiunile sociale și activitățile de agrement, fie acțiunile și sarcinile asociate cu ocupații profesionale, educaționale sau de alt fel, și chiar sarcini de rutină, inclusiv cumpărături online, efectuarea de plăți și chiar programarea angajamentelor și / sau îndeplinirea obligațiilor față de stat. Frecvența și intensitatea utilizării internetului și a TIC sunt, de asemenea, relevante.

Folosind conceptul de stil de viață online, care este cuprinzător, devine clar că nivelurile de risc de

victimizare informatică sunt diferite în funcție de activitatea desfășurată pe internet sau prin internet și TIC și pentru o utilizare de rutină diferită.

Unele activități, cum ar fi descărcarea de programe freeware[61] sau utilizarea site-urilor de partajare a fișierelor, prezintă un risc mai mare de victimizare cibernetică decât alte activități, cum ar fi verificarea e-mailurilor sau vizitarea canalelor de știri online. În mod similar, persoanele care se angajează în activități online mai puțin sigure, cum ar fi vizitarea site-urilor web necunoscute și / sau descărcarea de muzică, videoclipuri, filme și / sau jocuri pe platforme neoficiale, sunt mai susceptibile de a fi ținta unei forme de victimizare informatică (Choi, 2008, Moitra, 2005, Yar, 2005, 2006 cit în Yucedal, 2010). La rândul său, utilizarea unei camere web, utilizarea frecventă a cumpărăturilor online și acceptarea cererilor de prietenie pe rețelele sociale de la persoane / profiluri necunoscute măresc riscul de victimizare informatică, comparativ cu riscul de victimizare informatică evidențiat de persoanele fără un astfel de activități de rutină pe internet și cu TIC (Clarke, 2004 Van Wilsem, 2011; Butler, 2013).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

În ceea ce privește stilul de viață online și comportamentele de utilizare a internetului, este, de asemenea, important să rețineți că **persoanele cu experiențe personale de săvârșire sau implicare în criminalitate informatică prezintă, de asemenea, un risc mai mare de a se confrunta cu victimizarea informatică** (Choi, 2008, Wolfe și colab., 2008, Bossler & Holt , 2009, Van Wilsen, 2013 cit în Maimon & Louderback, 2019).

Acest risc crescut de victimizare de către persoane implicate în activități ilicite se regăsește în mod similar în infracțiunile tradiționale și este asociat cu stilul de viață, comportamentul și nivelurile diferite de expunere la circumstanțe, contexte și persoane / grupuri de risc (a se vedea rezumatul teoriilor criminologice în secțiunea 3.1 din acest manual).

În această chestiune și în cazul criminalității informatice, implicarea menționată anterior și apartenența la subculturi criminale specifice sunt asociate nu numai cu riscul de criminalitate informatică (Macdonald & Frank, 2017 cit în Maimon & Louderback, 2019), ci și cu cel al victimizării informatice, prin expunerea la semeni devianti.

Pentru a înțelege mai bine relevanța comportamentului în utilizarea internetului și a TIC și asocierea acestuia cu vulnerabilitatea la victimizarea informatică, este urgentă necesitatea de a aborda efectul de dezinhibare, o caracteristică importantă asociată cu utilizarea internetului și a TIC. Acest proces sau efect de dezinhibare rezultă din modul în care distanța fizică afectează interacțiunea sau comunicarea. Absența contactului direct în procesul de comunicare, anonimatul mai mare și percepția unui control mai mare asupra procesului de interacțiune par să contribuie la o schimbare mai ușoară a informațiilor, la exprimarea liberă a emoțiilor și gândurilor și la adoptarea unor comportamente care nu ar fi împărtășite. , exprimate și practicate în cazul interacțiunilor care au loc în contexte convenționale (Suler, 2004; Martellozzo & Jane, 2017). Acest efect dezinhibitor aparent avantajos poate contribui la expunerea la situații și / sau la adoptarea comportamentelor online care cresc vulnerabilitatea la victimizarea informatică (Agustina, 2015).

[61] Freeware se referă la software sau programe de calculator a căror utilizare nu necesită achiziționarea unei licențe / plată.

IMPORTANT | PRACTICA IN FOCUS:

În 1995, un grup de lucru al unei companii cu sediul în Statele Unite ale Americii a dezvoltat un memorandum numit *Netiquette Guidelines*, în care, pentru prima dată, a fost utilizat conceptul de ***netiquette***. A constat dintr-un set de reguli de comportament, inclusiv reguli de comunicare și standarde de securitate, aplicabile persoanelor și entităților colective, cu scopul de a asigura o utilizare sigură și adecvată a internetului și a diferitelor sale instrumente de comunicare.

Documentul original este disponibil la adresa https://www.ietf.org/rfc/rfc1855.txt .

În acest sens, este necesar să se sublinieze importanța **conștientizării, cunoașterii și abilităților de control în raport cu forma și tipul informațiilor personale** împărtășite sau care pot fi partajate pe internet și, în mod specific, pe rețelele sociale. În acest sens, a fost identificată o asociere semnificativă între percepția riscului de confidențialitate, controlul perceput cu privire la informațiile partajate și comportamentul de partajare a informațiilor pe rețelele sociale: persoanele cu niveluri mai ridicate de control perceput al informațiilor partajate / partajabile, împărtășesc mai atent, se percep pe sine ca fiind mai sigure și sunt mai puțin susceptibile de a fi victime ale criminalității informatice (Hajli & Lin, 2014 cit în Saridakis și colab., 2016).

3.3. Entitățile colective ca ținte ale criminalității informatice

Criminalitatea informatică are, de asemenea, potențialul de a afecta entitățile colective, trecând barierele victimizării individuale abordate în acest manual.

Ne referim în mod specific la situațiile în care țintele criminalității informatice sunt **corporații**, **multinaționale, instituții și chiar infrastructuri guvernamentale** (Yucedal, 2010; Näsi și colab., 2015).

Aceste entități pot suferi pierderi substanțiale ca urmare a criminalității informatice, fie din cauza pierderii clienților și / sau a informațiilor confidențiale compromise sau furate, fie prin pierderi financiare imediate, care pot chiar afecta și dăuna clienților individuali, precum și pierderilor viitoare, asociate cu o scăderea încrederii clienților în produsele și / sau serviciile pe care le furnizează (Nykodym, Taylor și Vilela, 2005, 2005; Kratchman și colab., 2008).

3. PERSPECTIVE CRIMINOLOGICE ȘI VICTIMOLOGICE PENTRU ÎNȚELEGEREA CRIMINALITĂȚII INFORMATICE

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Elementul uman este, de asemenea, important în criminalitatea informatică care vizează entitățile colective. Ne referim, și anume, la **rolul profesioniștilor și al personalului** acestor organizații și **la nivelurile lor de implementare a politicilor organizaționale și a măsurilor de protecție** împotriva criminalității informatice, precum și la comportamentele lor personale de auto-protecție a securității informatice.

Se știe că o înțelegere adecvată a vulnerabilităților organizaționale de către profesioniști și personal are un efect pozitiv asupra nivelului de conformitate cu strategiile și politicile de protecție adoptate de o anumită corporație sau organizație (Johnston & Warkentin, 2010 cit în Maimon & Louderback, 2019; Siponen și colab., 2010 cit în Maimon & Louderback, 2019).

Terorismul informatic, prezentat sumar în secțiunea 1 a acestui manual, este un exemplu al acestei criminalități informatice care vizează entitățile colective, întrucât intenția sa, așa cum s-a indicat anterior, se concentrează pe distrugerea și / sau incapacitarea infrastructurilor critice pentru funcționarea unei societăți sau a unui stat, și nu neapărat pe daunele aduse cetățenilor individuali (care pot apărea și în urma atacului).

De asemenea, în acest domeniu, este important de remarcat conceptul de hacktivism, care rezultă dintr-o intersecție între activismul politic și TIC, unde hacking-ul susține scopuri sau cauze politice (Yar & Steinmetz, 2019).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Anonymous, mișcarea internațională descentralizată a hacktivismului, care a apărut pe internet în anii 2000 și este cunoscută pentru practica sa de hacking și DDoS (a se vedea secțiunea 1.3 din acest manual pentru mai multe informații despre aceste forme de criminalitate informatică), a fost asociată cu mai multe atacuri împotriva infrastructurilor guvernamentale, multinaționalelor, instituțiilor financiare și entităților religioase.

Obiectivele acestor mișcări nu sunt clare, dar pretind că luptă împotriva cenzurii și opresiunii și în favoarea promovării libertății de exprimare.

4. COSTURILE ȘI IMPACTUL CRIMINALITĂȚII INFORMATICE

În această secțiune, vom acoperi un set de simptome și indicatori ai impactului victimizării informatice, cu avertismentul că, având în vedere multiplicitatea și vasta amploare a fenomenelor analizate, consecințele prezentate mai jos vor fi întotdeauna reductive și generice, ne-contemplând individualitatea fiecărei experiențe particulare și personale a victimizării informatice.

De asemenea, vom căuta să abordăm costurile financiare și economice asociate criminalității informatice, considerând că, deși acestea pot afecta direct și / sau indirect victime individuale, este comun ca consecințele lor să se reflecte și în costurile pentru entitățile colective, care sunt ținte atractive ale criminalității informatice.

4.1. Victimele criminalității informatice și consecințele experienței victimizării informatice

Impactul criminalității informatice asupra victimei este foarte variabil, fiind agravat sau atenuat în funcție de un set de variabile:

- **Variabile individuale**, și anume caracteristicile socio-demografice și abilitățile de utilizare a internetului (abordate deja în factorii de risc asociați cu victimizarea cibernetică în secțiunea 3 a acestui manual);
- **Variabile asociate cu criminalitatea informatică** în sine, inclusiv tipul de criminalitate informatică și nivelul de agresiune subiacentă, durata victimizării informatice, atingerea difuzării sau nivelul de publicitate al victimizării informatice și, acolo unde este cazul, relația cu autorul criminalității informatice (de exemplu, în situații de victimizare informatică în relațiile interumane);
- **Variabile asociate rețelei de asistență**, care include rețeaua formală de asistență (adică resursele și serviciile disponibile din justiție, sănătate, securitate și sisteme de securitate socială și ca organizații ale societății civile), precum și rețeaua informală de sprijin, și anume familia și prieteni.

4.1.1. Consecințe fizice, psihologice și emoționale

Studiile existente cu privire la impactul și consecințele victimizării cibernetice sunt rare și, cu puține excepții (de exemplu, Jansen și Leukfeldt, 2018), s-au concentrat în principal pe analiza impactului anumitor forme de criminalitate informatică, cum ar fi infracțiunile posibile de pe internet și TIC , posibil datorită componentei lor relaționale sau interpersonale.

În termeni generici, se consideră că consecințele suferite de victimele criminalității informatice nu sunt semnificativ diferite de consecințele suferite de victimele a ceea ce vom numi infracțiuni *tradiționale*. Consecințele și reacțiile adesea subliniate sunt: pierderea încrederii; vinovăție; rușine;

furie și frustrare; anxietate; frică și tristețe; sentimente de nesiguranță, neputință și dezamăgire (Leukfeldt și colab., 2019; Cross și colab., 2016; De Kimpe și colab., 2020). Impactul emoțional al anumitor tipuri de criminalitate informatică poate fi la fel de grav ca și consecințele financiare ale acestora (Modic și Anderson, 2015). Victimizarea poate schimba, de asemenea, modul în care victimele se percep pe sine și modul în care înțeleg și atribuie sens lumii din jur, inclusiv reducerea nivelurilor de încredere în sine și încredere în ceilalți (Jansen și Leukfeldt, 2018), și apoi pot evolua în efecte fizice cum ar fi insomnia, greața și / sau pierderea în greutate (Cross și colab., 2016).

În situațiile de stalking informatic, frica, suferința și îngrijorarea resimțite de victime sunt adesea identificate consecințe emoționale, psihologice și comportamentale (Holt & Bossler, 2008). Frica ar putea fi legată de autorul actelor de stalking informatic, dar ar putea fi asociată și cu frica de pierdere a reputației, datorită posibilității divulgării online a informațiilor personale și private și, ca atare, de a ajunge la un public numeros sau ridicat. niveluri de publicitate. Simptomatologia anxietății, inclusiv reexperimentarea incidentelor, și abuzul de substanțe sunt, de asemenea, asociate cu victimizarea stalking-ului informatic. Împreună cu consecințele emoționale și psihologice, pot apărea semne de stare de rău fizică, inclusiv somatizare, tulburări de somn, oboseală sau slăbiciune excesivă, probleme de apetit, dureri de cap și greață (Davies, Clark și Roden, 2016).

În cazurile de hărțuire informatică, putem enumera suferința, stima de sine scăzută, tristețea, furia, singurătatea și frustrarea, precum și tulburările somatice, depresia și ideația suicidară ca efecte negative frecvente asupra funcționării psihologice și emoționale a victimei. Bullying-ul informatic are, de asemenea, consecințe în funcționarea socială și educațională a copilului sau tânărului victimă și este asociat cu sentimente de ineficiență, izolare, absenteism școlar și scăderea performanței academice (Beran și Li, 2007; Mahmoud și Senosy, 2015; Wang și colab., 2011 cit în Arafa și colab., 2015).

Mai mult, studiile retrospective au identificat o gamă largă de consecințe negative din funcționarea emoțională și psihologică asociată cu abuzul sexual în copilărie, inclusiv: dificultăți educaționale și ocupaționale, agresivitate și implicare în activități criminale. În ceea ce privește situațiile de intimidare informatică, pot apărea situații de abuz sexual și simptome de exploatare a copiilor, cum ar fi frica, anxietatea, agresivitatea și iritabilitatea, precum și tulburările de somn și comportamentele regresive[62]. În mod similar, consecințele pot include, de asemenea, o scădere a performanței școlare, absenteismul școlar, precum și adoptarea unui comportament sexual inadecvat (Roopesh, 2016 cit în APAV, 2019).

În ciuda faptului că accentul pus pe abuzul sexual și exploatarea copiilor și consecințele acestora nu intră în sfera de aplicare a acestui manual, având în vedere natura atipică a unora dintre aceste situații, prezentăm mai jos un scurt rezumat al comportamentelor sexuale neadaptate menționate anterior care pot apărea ca consecințe / efectele expunerii la violența sexuală.

[62] Comportamentele regresive se referă la regresia în achizițiile de dezvoltare deja realizate de copil, care poate include, de exemplu, enureusis (pierderea involuntară a urinei), encopresis (defecație involuntară) și regresii de limbaj / comunicare.

[63] Pentru informații suplimentare detaliate despre violența sexuală împotriva copiilor, vă rugăm să consultați: APAV (2019). Manual de ÎNGRIJIRE - sprijin pentru copii și tineri victime ale violenței sexuale (ediția a II-a revizuită și extinsă). Lisabona: APAV.

Tabel 2: Comportamente sexuale care pot apărea ca o consecință a experiențelor de victimizare a violenței sexuale

Expresie sexualizată a afecțiunii

- Atingerea neadecvată a organelor sexuale ale altor copii și tineri (în special copii și tineri de vârste diferite de ale lor și / sau cu care copilul sau tânărul nu are o relație de încredere anterioară)
- Atingerea excesivă sau inadecvată a adulților
- Comportamente seducătoare față de persoanele adulte

Limbaj sexual timpuriu

- Utilizarea termenilor sexuali care indică cunoștințe neașteptate despre sexualitate pentru grupul lor de vârstă

Masturbare compulsivă și / sau comportament autoerotic extrem

- Masturbare persistentă chiar și atunci când i se solicită oprirea sau cenzurarea de către adulți (de exemplu, aplicarea unei pedepse consecvente pentru practicarea masturbării)
- Masturbare în locuri publice și / sau lângă alte persoane

Organizarea sau simularea unor episoade sexuale explicite și / sau interacțiuni

Comportament sexual care creează neliniște în sine și în ceilalți (în special la colegi)

- Comportamentul sexual provoacă durere fizică în sine și în colegii cu care încearcă să desfășoare acte sexuale
- Comportamentul sexual invadează viața privată a colegilor, este împotriva voinței lor și duce la reclamații ale colegilor

Comportamentul sexual conceput ca o formă de reciprocitate / apreciere a afecțiunii și / sau a bunurilor materiale

Preocupare constantă cu privire la sexualitate

Prin urmare, este clar că situațiile de abuz sexual și exploatare a copiilor prin intermediul internetului afectează dezvoltarea sănătoasă a acestora, inclusiv dezvoltarea sexuală, precum și identitatea acestora. Din cauza riscului ridicat de victimizare continuă asociat cu abuzul și exploatarea sexuală a copiilor, impactul experienței este probabil să crească în severitate și consecințele vor persista până la maturitate (Frothingham și colab., 2000 cit în Sigurjonsdottir, 2013).

De asemenea, în situațiile de discurs de ură online există un dublu impact: impactul conținutului / mesajului asupra victimei, dar și impactul care rezultă din mesajul de bază pe care același conținut este destinat să îl transmită (că victima și grupul de care aparține nu sunt tolerate de societate). Anonimatul pe care Internetul și TIC îl oferă infractorilor contribuie la perpetuarea agresiunii online și, astfel, intensifică suferința emoțională și psihologică a victimei. În plus, potențialul anonimatului de amplificare și „validare" socială, în special atunci când răspândirea are loc pe rețelele sociale, agravează și intensifică impacturile negative asupra funcționării emoționale, psihologice și chiar sociale a victimei (McGonagle, 2013).

În cazul infracțiunilor informatice, cum ar fi hacking-ul, spamul sau escrocheriile online, impactul asupra bunăstării emoționale și psihologice este subestimat în mare măsură și este de obicei discutat ca

infracțiuni cu impact redus (Button, Lewis și Tapley (2014a cit în Jansen & Leukfeldt, 2018). Cu toate acestea, dincolo de consecințele financiare asociate cu aceste forme de criminalitate informatică, există studii care indică apariția simptomelor de disconfort emoțional și psihologic, cum ar fi frica și anxietatea, precum și simptome fizice, cum ar fi problemele de somn și palpitații (Jansen și Leukfeldt, 2018).

4.1.2. Consecințe financiare

Daunele financiare suferite de victimele criminalității informatice depind în principal de formele de criminalitate informatică la care au fost supuse (Butler, 2013).

Prin urmare, pot exista consecințe financiare directe ale criminalității informatice, precum și consecințe indirecte, care pot include, de exemplu, alte costuri suportate de victime ca urmare a faptului la care au fost supuse, precum pierderea de timp, pierderea de ore de lucru, cheltuieli crescute cu costurile de sănătate, călătorii și telecomunicații, necesitatea înlocuirii echipamentelor IT și / sau nerespectarea acordurilor contractuale (Leukfeldt și colab., 2019). Există infracțiuni informatice ale căror consecințe pentru victimă includ și necesitatea de a-și schimba rutina, ceea ce poate implica adoptarea unor măsuri de protecție și implementarea unor mecanisme mai eficiente de securitate informatică, dar și schimbări mai semnificative în stilul de viață și activitățile zilnice, inclusiv mutarea casei, schimbarea locul de muncă / studiu sau altele, care implică în mod evident costuri financiare.

Pe de altă parte, costurile pe care entitățile le suportă ca răspuns sau consecință a faptului că sunt ținte de criminalitate informatică, un domeniu abordat în secțiunea 4.3 din acest manual, se reflectă în cele din urmă la nivel individual, asupra consumatorilor sau utilizatorilor online ai unui produs, bun sau serviciu dat (Das & Nayak, 2013).

4.1.3. Teama de criminalitatea informatică și riscul perceput de victimizare informatică

Frica de infracțiune poate fi definită ca o reacție emoțională la infracțiune și / sau la simbolurile asociate acesteia, în timp ce **riscul perceput** constituie o judecată cognitivă prin care oamenii își evaluează propriul risc sau probabilitatea de victimizare, pe baza experiențelor lor personale, a contextului social și a circumstanțelor , care la rândul său se reflectă în frica de infracțiune (Ferraro, 1995, Rontree, 1998 cit în Yucedal, 2010).

Rezultă că experiențele personale de victimizare pot crește riscul perceput de (re)victimizare și, în consecință, teama de infracțiune. Aceste procese cognitive nu sunt neapărat negative, deoarece pot promova adoptarea măsurilor și comportamentelor de siguranță și protecție (Rountree & Land, 1996, cit in idem).

Prin urmare:

- O persoană care a fost deja victima unei infracțiuni sau care se consideră expusă riscului de victimizare poate **adopta mai multe comportamente de siguranță și protecție**, inclusiv restricții în activitățile / interacțiunile sociale sau schimbări în rutina zilnică, precum și utilizarea instrumentelor și mecanismelor de protecție ;
- O persoană care a fost deja victimă a infracțiunilor se poate percepe ca **fiind expusă unui risc mai mare de (re) victimizare** și, în consecință, are niveluri mai ridicate de **frică de infracțiuni** decât persoanele fără experiență prealabilă de victimizare (Hindelang și colab., 1978, Cohen & Felson, 1979, Ferraro, 1995, Goodrum, 2007 cit in idem).

Aceste **procese cognitive de evaluare a riscului perceput de victimizare se aplică și victimizării informatice**. Riscul perceput de victimizare informatică, ca rezultat al proceselor cognitive care includ analiza experiențelor personale ale victimizării informatice anterioare (dacă este cazul) și a indicilor de victimizare / infracționalitate care decurg din stilul de viață online, poate duce la răspunsuri comportamentale care vizează protecție mai mare. Aceasta poate include punerea în aplicare a unor măsuri / mecanisme de securitate informatică (cum ar fi programe antivirus și firewall) și schimbarea comportamentelor de utilizare a internetului și a TIC (Yucedal, 2010).

În cele din urmă, riscul perceput de victimizare informatică are, de asemenea, un impact asupra nivelurilor de **vulnerabilitate la victimizarea informatică**, întrucât, la început, dacă o persoană se percepe pe sine ca fiind expusă riscului de victimizare informatică, va avea mai multe șanse să adopte comportamente și măsuri orientate către asigurarea securității informatică, care va contribui la reducerea riscului de victimizare informatică.

IMPORTANT | STATISTICA IN FOCUS:

Conform datelor din Eurobarometrul 423 menționat anterior, respondenții și-au exprimat **un nivel ridicat de îngrijorare cu privire la securitatea informatică și riscurile criminalității informatice**.

Iată câteva dintre principalele rezultate:

- Majoritatea (85% dintre respondenți) au fost de acord că **riscul de victimizare informatică este în creștere**.
- 73% dintre respondenți au fost îngrijorați de faptul **că informațiile lor personale online nu sunt păstrate în siguranță**.
- Tipurile de criminalitate informatică de care respondenții sunt cei mai preocupați sunt, în ordine descrescătoare: **furtul de identitate online** (68%), **malware** (66%), **escrocherii online** (între 56% și 63%), **hacking** (60%) și **spam** (57%). De asemenea, aproximativ jumătate dintre cei chestionați au fost îngrijorați de descoperirea accidentală a **materialelor de abuz și / sau exploatare sexuală a copiilor online** (52%) și de descoperirea accidentală a conținutului / materialului pentru **discursuri de ură** (46%).

În ciuda acestor îngrijorări, aproximativ 74% au declarat **că se pot proteja împotriva criminalității informatice**.

4.2. De la consecințe la nevoile victimelor criminalității informatice

În general, nevoile victimelor criminalității informatice sunt relativ similare cu nevoile victimelor altor forme de infracțiuni mai *tradiționale* și pot fi identificate diferite domenii ale nevoilor (Leukfeldt și colab., 2020).

În timp ce nevoile mai mult sau mai puțin comune victimelor oricărei forme de infracțiuni pot fi enumerate, vor exista nevoi specifice care diferă, de asemenea, în funcție de tipul de victimizare și de scara de timp (adică, nevoile unei victime ale criminalității informatice imediat după experiența criminalității informatice vor fi distinct de nevoile identificate la ceva timp după ce s-a produs criminalitatea informatică).

În plus, nevoile victimelor infracțiunilor depind și de caracteristicile personale ale victimei, de mediul lor social și de consecințele criminalității informatice specifice (Huang, 2018, Wood et al., 2015 cit in idem).

Tabelul de mai jos rezumă câteva dintre nevoile identificate de victimele criminalității informatice și care vor fi cauzate de experiența de victimizare informatică (Cross și colab., 2016; Leukfeldt și colab., 2020). Conținutul său nu este exhaustiv, având în vedere lipsa cercetărilor pe acest subiect.

Tabel 3: Nevoile identificate de victimele criminalității informatice

Nevoi emoționale și psihologice	Proceduri penale și nevoi legate de informații	Nevoi practice și financiare
• Recunoașterea ca victimă a unei infracțiuni • Recunoașterea experienței de victimizare informatică • Nevoia de a-și relata experiența și de a fi ascultate / ascultați • Recunoașterea externă (contexte și autorități sociale informale) a experienței victimizării informatice • Să beneficieze de asistență calificată și confidențială după experiența criminalității informatice • Recuperarea după consecințele emoționale și psihologice ale criminalității informatice • Acces la asistență profesională / calificată	• Informații despre resursele / structurile de sprijin existente și despre modul de solicitare a ajutorului • Sprijin în raportarea și formalizarea plângerii • Primește informații despre autorul criminalității informatice, ancheta și procesul • Primește informații despre rezultatul / rezultatul procedurilor penale • Reparația pentru infracțiune	• Sprijin cu eliminarea conținutului legat de criminalitatea informatică de pe Internet și TIC • Sprijin în legătura cu băncile, furnizorii de servicii de internet și alte platforme • Sprijin pentru restabilirea securității (păstrarea integrității fizice) și prevenirea revictimizării • Protecție / protejare împotriva autorului criminalității informatice • Nevoi financiare asociate cu activele / informațiile pierdute • Compensația monetară pentru pierderile cauzate de criminalitate informatică

Modul în care răspunsurile instituționale oferite de diferite sisteme și structuri, precum sistemul de justiție penală, sistemul de sănătate, sistemul de asistență socială și organizațiile societății civile,

intervin sau acționează, în vederea satisfacerii nevoilor victimelor infracționalității și, în special, victimele infracționalității informatice, pot da naștere **victimizării secundare**. Aceasta este a doua formă de victimizare, cauzată de răspunsul inadecvat oferit de aceste sisteme și structuri și de discrepanța acestora cu interesele, nevoile și drepturile victimelor.

Dificultățile diferitelor sisteme / servicii și structuri instituționale în a răspunde nevoilor victimelor criminalității informatice (*idem*) se pot datora următoarelor constrângeri:

- Resurse umane și materiale insuficiente;
- Ignorarea nevoilor și drepturilor victimelor sau a dificultăților structurale în implementarea acestora;
- Nevoia de instruire / cunoștințe specializate pentru contactarea și intervenția cu victimele criminalității informatice;
- Dificultăți asociate procesului penal, inclusiv identificarea unui suspect, formalizarea unei plângeri, anchetă și urmărire penală.

4.3. Costurile financiare și economice ale criminalității informatice

Criminalitatea informatică are diferite costuri pentru diferite entități, în special atunci când vizează entități colective. Amploarea costurilor economice și financiare ale criminalității informatice variază în funcție de sector, dimensiunea organizației, activele informaționale și severitatea formei (formelor) de criminalitate informatică utilizată (Gañán, Ciere & van Eeten, 2017).

Criminalitatea informatică, atunci când sunt vizate entități colective, și anume corporații și organizații, își propune, în special în cazul entităților mai mari, să compromită activele lor informaționale. Pe de altă parte, entitățile mai mici par a fi ținte mai puțin atractive pentru criminalitatea informatică (Gañán și colab., 2017).

Cu toate acestea, atunci când vorbim despre costurile economice și financiare ale criminalității informatice pentru entități, multe dintre aceste efecte sunt **efecte intangibile** și nu tocmai pierderea de bani reali. În timp ce necesitatea unor estimări monetare cuprinzătoare este de înțeles, impactul economic și financiar al criminalității informatice este dificil de măsurat, întrucât unele dintre efecte pot fi monetizate pe baza datelor empirice disponibile, dar multe dintre ele nu sunt (*idem*).

Diferitele tipuri de costuri asociate criminalității informatice pot fi clasificate drept costuri în anticiparea criminalității informatice, ca o consecință a criminalității informatice și ca răspuns la criminalitatea informatică (*idem*).

Astfel, costurile anticipate și costurile în consecință pot include costurile (înainte și / sau după) cu **identificarea riscurilor**, construirea **procedurilor de operare a securității informatice** și

achiziționarea de software și hardware de **protecție împotriva criminalității informatice**. Aceste costuri pot include, de asemenea, consultanță de specialitate în domeniul securității informatice, precum și costuri asociate cu testarea, monitorizarea și actualizarea regulată a riscurilor, procedurilor și sistemelor de securitate informatică (Das și Nayak, 2013).

Costurile de răspuns vor include toate **cheltuielile și eforturile din sectorul public sau privat în lupta împotriva criminalității informatice**, suportate și de societate, inclusiv costurile asociate cu contribuțiile sistemului de justiție penală pentru investigarea și combaterea criminalității informatice (Gañán și colab., 2017).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Impactul criminalității informatice asupra încrederii utilizatorilor

Costurile de anticipare sunt cruciale pentru a asigura încrederea și securitatea utilizatorilor și consumatorilor pe internet și TIC.

Confortul, accesibilitatea și securitatea asociate cu utilizarea internetului și a TIC pentru consumul și achiziționarea de produse, bunuri și servicii stau la baza preferinței consumatorilor pentru comerțul electronic și activitățile online, comparativ, de exemplu, cu magazinele fizice .

Criminalitatea informatică subminează avantajele asociate cu utilizarea internetului și a TIC, crescând **indicii de risc percepuți** de utilizatorii și consumatorii online, reducând nivelurile de încredere și contribuind astfel la schimbarea atitudinilor față de consumul online.

Dacă percepția riscului față de criminalitatea informatică subminează încrederea utilizatorilor sau a consumatorilor în utilizarea internetului și a TIC pentru anumite activități, atractivitatea platformelor online pentru consumul și achiziționarea de produse, bunuri și servicii scade, ceea ce la rândul său se poate schimba online obiceiuri și comportament (Saban, McGivern & Saykiewicz, 2002; Smith, 2004; Saini, Rao și Panda, 2012).

PARTEA II
INTERVENȚIA

PARTEA II

INTERVENȚIA

1. ROLUL SPECIALIȘTILOR ÎN OFERIREA DE SPRIJIN PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

Acest capitol abordează importanța și rolul specialiștilor care sprijină victimele criminalității informatice și competențele și abilitățile necesare pentru îndeplinirea acestor funcții. De asemenea, explorăm riscurile psihosociale ale intervenției cu victimele infracțiunilor, concentrându-ne pe victimele criminalității informatice.

1.1. Competențe personal

Sprijinirea victimelor infracțiunilor, în special a criminalității informatice, necesită un set de abilități esențiale de sprijin specializat.

Competențele personale se referă la caracteristicile personale și personalitatea specialistului și la modul în care acestea se potrivesc cu funcțiile și sarcinile de sprijin. Acestea sunt esențiale în orice profesie de îngrijire și, prin urmare, sunt deosebit de importante pentru specialiștii care lucrează în contact direct cu și susțin persoanele aflate în dificultate sau în criză (APAV, 2013b), precum victimele criminalității informatice.

Principalele competențe profesionale pentru sprijin și intervenție în ceea ce privește victimele infracțiunilor - cum ar fi empatia, deschiderea și disponibilitatea - sunt abordate mai jos (Pessoa, din Mota Matos, Amado & Jäger, 2011).

În plus, **specialistul ar trebui să fie capabil să gestioneze și să stabilească relații interpersonale pozitive** atunci când sprijină victimele infracțiunilor. Aceasta include contactul și interacțiunea cu victimele, rudele și prietenii acestora, precum și stabilirea de legături cu profesioniștii și organizațiile partenere implicate în sprijinul și intervenția în ceea ce privește victima. Această dimensiune relațională - gestionarea relațiilor umane - include capacitatea de **rezolvare pașnică a problemelor interpersonale și / sau interinstituționale și gestionarea pozitivă a stresului**. Aceștia sunt indicatori buni ai capacității de relaționare cu ceilalți, în special într-o intervenție atât de complexă și solicitantă, unde specialistul se poate confrunta cu adversități constante (APAV, 2013b; APAV, 2017).

În mod similar, **autogestionarea emoțională** este, de asemenea, o competență cheie - aceasta este capacitatea de a gestiona și de a regla emoțiile cuiva în situații stresante, frustrante și solicitante, care sunt diferite de viața de zi cu zi (APAV, 2013b). Contactarea și desfășurarea intervențiilor cu victimele infracțiunilor implică niveluri ridicate de implicare emoțională, care trebuie declanșate rapid pentru a face față experiențelor de violență / infracțiuni împărtășite de victime, pentru a oferi sprijin (și pentru a face față stresului și frustrării asociate fiecărui caz)) și pentru a face față impacturilor asupra echilibrului emoțional al specialiștilor (APAV, 2017).

Specialistul ar trebui să demonstreze, de asemenea, **toleranță și respect pentru valorile și diferențele culturale**: indiferent de caracteristicile sau atitudinile oricărei victime, abordarea specialistului ar trebui să fie întotdeauna deschisă și acceptantă. Neutralitatea și imparțialitatea sunt fundamentale pentru a oferi sprijin eficient, iar specialiiștii ar trebui să încerce să-și gestioneze și

să-și controleze valorile și convingerile personale atunci când susțin orice victimă (*idem*). Legat de această dimensiune, la baza oricărui proces de sprijin acordat victimelor infracțiunilor, este **respectul pentru demnitatea umană** și este fundamental să acceptați necondiționat victima ca ființă umană, în același timp asemănătoare cu dumneavoastră, dar și ca unică și individuală.

Nu în ultimul rând, este important să menționăm două dimensiuni de bază atunci când contactăm și sprijinim victimele oricărei infracțiuni:

- **Compasiune și Empatie:**

  Abilitatea de a se pune în locul celuilalt sau de a se imagina ca acea persoană în acea situație este fundamentală atunci când contactează, susține și susține intervenții cu victimele oricărei infracțiuni. Capacitatea de a vedea lucrurile din perspectiva victimei, de a fi sensibil(ă) la situația trăită de victimă și de a simți și înțelege sentimentele și semnificațiile victimei atribuite infracțiunii sunt importante în stabilirea unei relații de susținere și încredere între specialist și victimă și pot fi un ajutor important pentru succesul sprijinului și / sau intervenției.

  Empatia nu înseamnă că specialistul ar trebui să plângă sau să fie mișcat de ceea ce descrie victima despre situația infracțională; ceea ce este important este capacitatea specialistului de auto-gestionare emoțională. Acest echilibru este foarte important, deoarece ajută victima infracțiunii să recunoască specialistul ca punct de referință, ca persoană pregătită și calificată pentru această activitate (APAV, 2017; APAV 2019).

- **Vocația:**

  Aceasta este mai degrabă o condiție personală decât o competență – îmbrățișarea valorilor solidarității sociale este foarte importantă pentru implicarea în sprijin, informare și / sau intervenție în ceea ce privește victimele oricărei infracțiuni (APAV, 2017).

1.2. Competențe tehnice de bază și specifice

În plus față de competențele personale menționate mai sus, specialistul care contactează și oferă asistență victimelor infracțiunilor și, în special, victimelor criminalității informatice, trebuie să fie calificat corespunzător în acest scop și pentru aceste funcții. Profesionistul ar trebui, de asemenea, să fie încorporat într-o anumită instituție, fie ea publică sau privată, guvernamentală sau neguvernamentală, voluntariat social sau nu (APAV, 2013b).

Formarea de bază (adică calificările academice) într-un anumit domeniu științific (cum ar fi științele sociale, de exemplu, sau într-un alt domeniu, în funcție de tipul de sprijin oferit de specialist și / sau organizația de sprijin) și **experiența profesională** acumulată sunt cerințe importante pentru intervenția

cu victimele oricărei infracțiuni, inclusiv a criminalității informatice, în diferitele sale forme (APAV, 2017).

Astfel, este de așteptat ca, în funcție de nevoile victimei identificate și de natura sprijinului solicitat, anumiți specialiști să fie mai potriviți pentru a satisface cel mai bine interesele, nevoile individuale și drepturile diferitelor victime ale infracțiunilor. Prin urmare, este clar că, de exemplu, sprijinul juridic ar trebui să fie oferit de profesioniști specializați în domeniul dreptului, iar sprijinul psihologic ar trebui să fie oferit de psihologi calificați[64].

De asemenea, este important să subliniem faptul că, având în vedere diversitatea nevoilor și consecințelor resimțite de obicei de victimele criminalității informatice[65], există o **cerință de sprijin și intervenție interdisciplinară**. care poate implica acțiunea profesioniștilor provenind din medii tehnice diferite, precum și intervenția diferitelor organizații. O abordare bazată pe rețea care implică profesioniști și organizații cu expertiză și *know-how* diferite și din diferite domenii / sectoare de intervenție contribuie la o mai bună intervenție cu fiecare victimă a criminalității informatice și la satisfacerea adecvată a nevoilor lor individuale.

Pe lângă învățământul superior și experiența profesională, specialistul care contactează sau sprijină victimele criminalității informatice ar trebui să aibă, de asemenea, o **pregătire specifică**, regulată și continuă în intervenția cu victimele infracțiunilor și criminalității informatice, precum și criminalitatea informatică ca domeniu specific de cunoaștere (APAV, 2013b ; APAV, 2017). În cadrul acestei formări specifice, ar trebui luate în considerare următoarele conținuturi cheie: înțelegerea teoretică, criminologică și victimologică a diferitelor forme de criminalitate informatică; cunoștințe despre consecințele, impacturile și dinamica criminalității informatice, precum și despre nevoile și drepturile victimelor; cadrul legal și răspunsurile juridice și sociale existente; securitate informatică; printre alte conținuturi.

În plus, având în vedere natura criminalității informatice și mecanismele împotriva cărora (sau prin care) este comisă, contactarea și susținerea victimelor criminalității informatice necesită, de asemenea, **cunoștințe și formare specializată cu privire la internet, TIC și alte echipamente**, atât în ceea ce privește modul în care acestea funcționează, cât și instrumente de comunicare folosite pe internet (care includ rețelele sociale) și în ceea ce privește modul în care pot fi utilizate pentru comiterea infracțiunilor și / sau modul în care pot fi ele însele ținte ale criminalității informatice (Bloom, 2007, Poh și colab., 2013, Trepal și colab. al., 2007, Mallen, Vogel și Rochlen, 2005 cit în APAV, 2017). **Competența informațională și tehnologică** a specialiștilor este fundamentală pentru capacitatea lor de a urmări evoluția constantă a TIC, tendințele de comunicare prin Internet, precum și mutația permanentă și consecventă a criminalității informatice.

Nu mai puțin importante sunt **abilitățile de comunicare** în contactarea și susținerea victimelor criminalității informatice, și anume a ști cum să asculți, dar și capacitatea de a transmite informații și mesaje clare și inteligibile, ca parte a procesului de sprijin, în jurul unor subiecte destul de complexe (Person și colab., 2011). Comunicarea și empatia, ca bază a procesului de sprijin și a relației dintre specialiști și victimele criminalității informatice, vor fi tratate mai detaliat în următoarele secțiuni ale acestui manual.

[64] Vezi Partea II, Capitol 3, secțiunea 3.5 al acestui manual pentru informații privind aspectele cheie ale sprijinului specializat acordat victimelor infracțiunilor cibernetice.

[65] Vezi Partea I, Capitol 4 al acestui manual pentru mai multe informații despre acest subiect.

1.3. Riscuri psihosociale din contactarea și sprijinirea victimelor criminalității informatice

Profesioniștii care contactează, susțin și/sau furnizează intervenții pentru victimele infracțiunilor prezintă niveluri ridicate de **oboseală fizică și emoțională, suferință psihologică și stres profesional** - acest lucru se datorează acestor funcții și necesității contactului direct cu persoanele aflate în situații de vulnerabilitate și fragilitate deosebite (emoțională și, de asemenea, fizică) cauzate de victimizare și victimizare informatică. Nu numai că acești specialiști sunt expuși experiențelor personale de victimizare ale altor persoane, dar sunt confruntați și cu frustrările asociate dezechilibrului dintre așteptările de soluționare/abordare a problemelor și nevoilor prezentate de victimă și funcționarea și resursele oferite de sistem. și de structurile instituționale. În plus, pentru profesioniștii care susțin victimele criminalității informatice, dincolo de expunerea *convențională* la raportarea victimelor despre experiențele lor personale de victimizare (a se vedea următoarele secțiuni din acest manual, unde vom detalia importanța colectării informațiilor), o altă dimensiune potențial stresantă sau traumatică se referă la necesitatea de a vizualiza conținut, cum ar fi imagini, fotografii și/sau videoclipuri, de natură infracțională asociată cu formele de criminalitate informatică comise împotriva victimei care este susținută. Acest conținut poate avea un caracter marcat agresiv, violent și chiar explicit sexual și are loc atunci când, de exemplu, sunt sprijiniți copiii și tinerii victime ale abuzurilor și/sau exploatării sexuale prin intermediul internetului, victimele hărțuirii online sau victimele șantajului sexual sau diseminarea non-consensuală a imaginilor și videoclipurilor, de exemplu, în situații de distribuire fără consimțământ a unor imagini intime[66]). Expunerea continuă la acest tip de conținut potențial traumatic poate afecta bunăstarea și sănătatea mintală a specialiștilor de sprijin (McCann și Pearlman, 1990).

Prin urmare, nu este neobișnuit să apară epuizarea, care este definită succint ca un sindrom (sau constelație de simptome), care include simptome **de epuizare emoțională, depersonalizare**[67] și **împlinire personală scăzută**, ca răspuns la situații de muncă stresante (Campos, Jordani , Zucoloto, Bonafé & Maroco, 2012).

Tabelul următor rezumă câteva măsuri organizatorice preventive și comportamente individuale atunci când contactați sau susțineți victimele criminalității informatice, în vederea prevenirii riscurilor psihosociale asociate sprijinirii victimelor infracțiunilor și criminalității informatice.

[66] Pentru informații detaliate despre aceste forme de criminalitate cibernetică, vă rugăm să consultați partea I, capitolul 1 al acestui manual.

[67] Depersonalizarea este definită ca procesul de dezumanizare în tratamentul / contactul cu celălalt, manifestat prin interacțiuni interumane lipsite de afectivitate și empatie.

1. ROLUL SPECIALIȘTILOR ÎN OFERIREA DE SPRIJIN PENTRU VICTIMELE CRIMINALITĂȚII INFORMATICE

Tabel 1: Măsuri de prevenire a riscurilor psihosociale asociate sprijinirii victimelor infracțiunilor și criminalității informatice

Măsuri organizaționale ale entității ce oferă serviciul de sprijin	Comportamente individuale ale specialistului care oferă sprijin
• Promovarea unei culturi organizaționale a deschiderii către feedback și către schimbul de experiențe • Oferirea de acces specialiștilor la mecanisme sau răspunsuri de sprijin psihologic intern și / sau extern • Implementarea de mecanisme de consiliere (livrare individuală sau de grup) pentru a promova bunăstarea specialiștilor de sprijin • Organizarea de întâlniri periodice pentru a discuta și a împărtăși experiențe / cazuri între colegi / echipă / specialiști de sprijin • Asigurați-vă că spațiile de lucru sunt echipate cu resurse materiale și logistice necesare activităților de lucru și pentru promovarea bunăstării • Promovarea de activități recreative și de agrement care nu sunt legate de sarcinile și funcțiile obișnuite de lucru	**Comportament de auto-îngrijire:** • Exerciții fizice • Activități de agrement • Respectarea standardelor de bază de sănătate și menținerea unei diete echilibrate și o igienă bună a somnului • Păstrarea legăturii cu familia și prietenii • Recunoașterea și respectarea limitelor corpului și minții • Asigurarea perioadelor de odihnă și deconectare de la locul de muncă, prin activități plăcute • Folosirea tehnicilor de relaxare și meditație • Contactul cu natura **Tehnici de intervenție:** • Acces la asistență psihologică, oferită de organizația de asistență, fie intern sau extern • Participarea la consiliere individuală și / sau de grup (echipă / perechi)

2. ASPECTE CHEIE PENTRU CONTACTELE INIȚIALE CU VICTIMELE INFRACȚIUNILOR INFORMATICE

Acest capitol acoperă un set de linii orientative generale pentru contactele inițiale cu victimele criminalității informatice, un pas care are loc înainte de o intervenție mai structurată și de calitate și ar trebui să se aplice oricărei organizații care contactează victimele criminalității informatice.

În acest scop, subliniem dimensiunile cheie pentru stabilirea unei relații de încredere între victimă și specialistul de sprijin, inclusiv comunicarea și empatia, dar și colectarea de informații și modul în care va ghida orice intervenție ulterioară cu victima criminalității informatice. Acest capitol se încheie cu o abordare a îngrijirii copiilor și tinerilor victime ale criminalității informatice, având în vedere vulnerabilitatea lor specială.

2.1. Orientări generale pentru contactele inițiale cu victimele criminalității informatice

Căutarea de sprijin poate reprezenta pentru o victimă a criminalității informatice un moment cheie și determinant a recuperării emoționale și psihologice și pentru restabilirea normalității în viața sa.

Cu toate acestea, la fel ca în alte infracțiuni și, de asemenea, în situații de criminalitate informatică, doar o mică parte din victime, a căror număr exact nu este cunoscut, aleg să caute sprijin formal, în special din partea răspunsurilor și serviciilor de sprijinire a victimelor. În ciuda reticenței frecvente de a căuta sprijin (Cross et al., 2016), din motive care se intersectează cu cele care nu raportează criminalitatea informatică[68], de regulă, cererea de sprijin va depinde de două condiții: ca victimele criminalității informatice să se recunoască ca victime ale unei infracțiuni și să evalueze criminalitatea informatică suferită ca fiind gravă (De Kimpe și colab., 2020).

Vă prezentăm mai jos câteva orientări globale pentru acțiunile specialiștilor atunci când susțin victimele oricărei infracțiuni, inclusiv victimele criminalității informatice (Winkel, 1991; Machado și Gonlçalves, 2003 cit în APAV, 2013b; Cross, Richards & Smith, 2016; Wedlock & Tapley, 2016 ; De Kimpe, Ponnet, Walrave, Snaphaan, Pauwels & Hardyns, 2020).

[68] Consultați Partea I, Capitolul 1, Secțiunea 1.4 din acest manual pentru informații mai detaliate despre diferența dintre criminalitatea cibernetică raportată și cea comisă efectiv.

2. ASPECTE CHEIE PENTRU CONTACTELE INIȚIALE CU VICTIMELE INFRACȚIUNILOR INFORMATICE

Tabel 2: Linii directoare generale pentru contactele inițiale cu victimele criminalității informatice

Obiective	Atitudini
Confirmă primirea reclamației / raportului	Recunoașteți curajul victimei de a căuta sprijin și de a dezvălui experiența sa personală de victimizare informatică.
Respectați ritmul victimei și încurajați împărtășirea experiență	Utilizați de preferință întrebări deschise, precum „ce aveți să ne spuneți?", promovând un spațiu / context sigur pentru împărtășirea liberă de informații. Respectați și promovați ventilarea emoțională, precum și momentele de fragilitate și emoționalitate mai mari asociate cu împărtășirea experienței criminalității informatice. Clarificați / puneți întrebări, fără presiune, atunci când informațiile furnizate de victimă sunt neclare sau insuficiente. Respectați momentele, pauzele și tăcerile victimei, inclusiv ezitările în împărtășirea informațiilor.
Validați experiența	Ascultați empatic, demonstrând că ascultați și înțelegeți ceea ce se spune și prețuind reacțiile, emoțiile / sentimentele, comportamentele, gândurile și semnificațiile atribuite de victimă experienței sale de victimizare / victimizare informatică. Demonstrați că credeți ceea ce vă spune victima despre ceea ce i s-a întâmplat, fără a judeca asta. Normalizați reacțiile victimei.
Restabiliți controlul	Oferiți informații clare, concentrându-vă pe informațiile esențiale pentru victimă despre ceea ce s-a întâmplat și pașii următori de adoptat, printr-un limbaj simplu și clar, ajustat la caracteristicile victimei. Nu preluați luarea deciziilor în locul victimei, acceptați deciziile victimei fără a le judeca și susțineți implementarea / activarea acestora, astfel încât victima să poată restabili controlul asupra vieții sale. Respectați alegerile victimei.
Demontați idea "vulnerabilității unicat"	Oferiți informații despre infracțiune și prevalența acesteia.
Preveniți învinovățirea	Nu criticati. Încadrați reacțiile victimei în contextul emoțional asociat cu infracțiunea. Apreciați încercările de protecție anterioare, chiar dacă acestea ar fi fost ineficiente. Evitați să folosiți expresii precum „de ce nu ..." și „ar fi trebuit să ...".
Preveniți evitarea și izolarea	Recomandați reluarea progresivă a activităților, inclusiv a obiceiurilor de utilizare a internetului și a TIC. Încurajați o implicare sporită în activități plăcute anterior, în special activități offline. Mobilizați sprijinul social. Evitați supra-protejarea de către familie și prieteni (fără a neglija siguranța victimei).
Promovați procesarea emoțională și cognitivă a experienței	Nu sfătuiți victima să „uite totul" și sfătuiți persoanele apropiate să nu facă acest lucru. Sugerați victimei să își împărtășească sentimentele și temerile cu cei în care are încredere, sfătuindu-i pe cei apropiați victimei să rămână la dispoziția sa pentru a asculta, fără a pune presiune pe victimă să-și împărtășească experiența.
Preveniți noi infracțiuni	Discutați despre strategiile de securitate și securitate informatică. Creșteți gradul de conștientizare a riscurilor asociate cu utilizarea internetului și a TIC prin promovarea implementării mecanismelor de securitate informatică și adoptarea comportamentelor de protecție personală atunci când se utilizează internetul și TIC. Elaborați, dacă este necesar, un plan de protecție cu victima (în special în situațiile în care victimizarea informatică este însoțită de victimizare în contexte *tradiționale*).
Implicați persoane importante în procesul de recuperare	Dacă victima este dispusă și cu permisiunea lor, implică familia și / sau prietenii în procesul de recuperare, solicitându-le ajutorul pentru a sprijini procesarea experienței și pentru a preveni noi infracțiuni, evitarea și izolarea.

De asemenea, prezentăm mai jos o sistematizare a bunelor practici și a greșelilor obișnuite de evitat în contactul cu orice victimă a unei infracțiuni (APAV, 2019b).

Tabel 3: Bune practici *vs* greșeli de evitat în contactul cu victimele criminalității informatice

Bune practici în contactul cu victima criminalității informatice	Greșeli de evitat în contactul cu victima criminalității informatice
Să credeți relatarea victimei.	Să nu credeți relatarea victimei.
Încurajați victima să vorbească despre situația de victimizare informatică, dar fără a pune presiune asupra sa.	Preluarea procesului decizional de la victimă, o eroare identificabilă de obicei prin expresii precum „Nu ar trebui ...", „Trebuie ...".
Respectați confidențialitatea, ținând cont de limitele sale.	Luarea deciziilor fără acordul prealabil al victimei.
Nu judecați.	Oferirea victimei a unui fals sentiment de securitate, promovarea așteptărilor nerealiste cu privire la rolul specialistului, la rezolvarea situației sau la nevoile victimei, care pot fi identificate prin verbalizări precum „Nu vă faceți griji. Totul va fi bine".
Respectați interpretarea victimei asupra situației sale specifice, chiar dacă aceasta diferă de punctul de vedere al specialistului.	Minimizarea problemei și a impactului acesteia.
Normalizați experiența de victimizare informatică și reacțiile, emoțiile, sentimentele și gândurile asociate.	Adoptarea unei poziții de hiper-protecție față de victimă.
Explicați-i victimei că există alte persoane care se confruntă cu situații similare, rupând percepția de a fi un „caz unic".	Demonstrarea un interes excesiv pentru detaliile despre victimizarea informatică pe care victima nu dorește să le dezvăluie (sau nu este încă pregătită să le dezvăluie în acel moment).
Transmiteți victimei că nu este responsabil(ă) pentru situație, ajutând-o să facă față posibilelor sentimente de vinovăție față de sine.	Arătarea de puțin timp și / sau disponibilitate victimei și pentru ascultare, de exemplu, prin manifestări non-verbale de neliniște și / sau întreruperi ale discursului său.
Pentru a ajuta victima în procesul de luare a deciziilor, arătați-i avantajele și dezavantajele fiecărei opțiuni pentru a sprijini luarea deciziilor în cunoștință de cauză.	Propunerea de interpretări sau diagnostice pentru reacțiile, emoțiile / sentimentele și gândurile victimei în legătură cu experiența sa de victimizare informatică, care poate fi transmisă în expresii precum „Faceți asta pentru că ...".
Evaluați riscul de (re)victimizare informatică și nevoile victimei, oferiți sprijin adecvat, în funcție de situația sa, și / sau trimiteți-o către serviciile și / sau organizațiile care oferă sprijin.	Oferirea de soluții, fără a implica victima în procesul decizional.
Fiți pregătit(ă) să interveniți într-o situație de criză.	Folosirea umorul în mod necorespunzător sau oferirea de auto-revelații inutile ca strategii pentru stabilirea unei relații de încredere.

2.2. Importanța comunicării și empatiei

Empatia, așa cum s-a menționat mai sus, se caracterizează prin capacitatea de a înțelege perspectiva celuilalt și de a percepe și de a înțelege sentimentele sale actuale, ceea ce au simțit atunci când s-au confruntat cu victimizarea informatică, ceea ce au crezut sau au gândit despre eveniment, precum și capacitatea de a demonstra înțelegerea și validarea reacțiilor precum disconfort și neliniște sau altele,

urmând, mai mult sau mai puțin imediat, după criminalitatea informatică.

Empatia specialistului față de victimă și experiența sa de victimizare informatică este foarte importantă pentru **stabilirea unei relații de sprijin și încredere între specialist și victimă** și este fundamentală pentru implementarea cu succes a obiectivelor enumerate mai sus (a se vedea Tabelul 2).

Având un **rol crucial în comunicarea umană**, deoarece facilitează procesul de comunicare, empatia încurajează victima să împărtășească, inclusiv informații și dovezi, care vor contribui la succesul procesului de sprijin, la recuperarea victimei și la satisfacerea nevoilor acesteia, dar și în beneficiul procedurile penale (De Vignemont & Singer, 2006; Sommers-Flanagan & Sommers-Flanagan, 2014, Themeli, 2014, Morrison, 2014 cit în APAV, 2018).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Empatia nu poate însemna însă că specialistul își pierde controlul de sine și plânge cu victima. O astfel de conduită sau reacție poate provoca, chiar dacă din greșeală, un impact negativ asupra victimei și asupra calității procesului de sprijin, deoarece victima nu mai poate înțelege specialistul ca pe cineva calificat și pregătit să ofere sprijin.

Unele dintre aspectele pe care specialistul ar trebui să le ia în considerare în comunicarea empatică sunt (APAV, 2019b):

- Mențineți contactul vizual cu victima, într-un mod calmant, nu curios.
- Însoțiți contactul vizual cu un ton de voce senin și interesat și cu limbajul corpului care arată disponibilitatea și liniștea (de exemplu, evitând să priviți ceasul, să arătați orice semn de nerăbdare sau să efectuați întreruperi inutile discursului victimei).
- Folosiți interjecțiile care întăresc și validează ceea ce împărtășește victima din experiența sa de victimizare informatică și curajul său în căutarea de sprijin.
- Demonstrați în mod clar că ascultați cu atenție informațiile pe care le împărtășește victima, inclusiv prin limbaj nonverbal (dând din cap, de exemplu).
- Asigurați victima că înțelegeți informațiile pe care le împărtășește, de exemplu, prin:
    - Reformulări - repetați cu propriile cuvinte conținutul transmis de victimă. Reformularea îl ajută pe specialist să se asigure că a înțeles în mod corespunzător victima, dar, de asemenea, asigură / informează indirect victima că este ascultată cu atenție, ceea ce o va încuraja să continue.
    - Rezumate - rezumă informațiile împărtășite de victimă, și anume la închiderea unui subiect, la sfârșitul unei sesiuni de sprijin și / sau la începutul celei următoare. Rezumarea poate fi o modalitate excelentă de a închide lacunele de informații și / sau dezacordurile cu privire la ceea ce a fost raportat de fapt.
- Asigurați-vă victima că sunteți interesat(ă) și că sunteți implicat(ă) în contact / interacțiune, adresând întrebări, de exemplu. Scopul unui echilibru între întrebări deschise și închise, care

facilitează comunicarea spontană și împiedică victima să se simtă interogată. Când abordați subiecte noi și pentru a promova împărtășirea de informații din partea victimei, alegeți întrebări deschise. Pe de altă parte, utilizați întrebări închise pentru a obține informații concrete și specifice.
- Încurajați exprimarea emoțională, mai ales atunci când persoana este în criză. Cu toate acestea, profesionistul nu ar trebui să impună exprimarea emoțională dacă victima nu și-a exprimat dorința de a face acest lucru.

2.3. Colectarea de Informații ca un pas cheie

Colectarea informațiilor este un proces central pentru susținerea și intervenția oricărei victime a infracțiunilor, inclusiv a victimelor criminalității informatice.

Primul contact cu victima va fi dedicat acestui proces de colectare a informațiilor despre criminalitatea informatică, impactul acesteia și nevoile declanșate. Cu toate acestea, este important să rețineți că **colectarea și analiza informațiilor sunt pași circulari și constanți**, care alimentează în mod regulat orice proces de sprijin și intervenție privind victimele infracțiunilor și ale criminalității informatice.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Nu este neobișnuit ca victima să prezinte **semne de anxietate și disconfort în acest prim contact cu specialistul de sprijin** și / sau organizația care oferă sprijin.

Specialiștii ar trebui să considere că victima poate, pentru prima dată, să împărtășească informații despre situația lor de victimizare informatică și este normal să prezinte semne de disconfort, suferință și fragilitate, ezitare și / sau rușine. Acești indicatori pot fi deosebit de prevalenți atunci când informațiile care trebuie împărtășite conțin orice fel de detalii legate de intimitatea relațională și / sau sexuală a victimei.

Specialistul ar trebui (în conformitate cu informațiile rezumate în Tabelul 2):

- Să respecte tăcerile, ezitările și ritmul victimei.
- Să consolideze curajului victimei în căutarea de sprijin și schimbul de informații despre istoricul victimizării informatice.
- Să explice și să asigure victima că reacțiile, emoțiile / sentimentele și gândurile sale sunt normale, atât în ceea ce privește disconfortul la împărtășirea de informații într-un context de susținere, cât și în ceea ce privește experiența în sine a victimizării informatice: în orice caz, acestea sunt reacții naturale la evenimente și circumstanțe neașteptate sau anormale din viață.
- Să demonstreze disponibilitatea și dorința de a susține și asculta victima, inclusiv temerile, preocupările și dorințele sale.

Colectarea informațiilor ar trebui să fie adaptată la starea emoțională a victimei, ceea ce înseamnă că, dacă victima nu este în măsură să furnizeze toate informațiile, specialistul ar trebui să colecteze cât mai multe informații posibil și, dacă acest lucru nu este suficient, contactele de îngrijire ulterioare ar trebui să fie programate pentru a permite colectarea de informații mai cuprinzătoare.

Trebuie acordată prioritate bunăstării emoționale a victimei, chiar în detrimentul necesității de a colecta informații.

2. ASPECTE CHEIE PENTRU CONTACTELE INIȚIALE CU VICTIMELE INFRACȚIUNILOR INFORMATICE

Pe scurt, colectarea de informații de la victima criminalității informatice permite specialistului de asistență să:

1

- obțină informații despre situația criminalității cibernetice trăite de victimă
- evalueze impactul și consecințele suferite de victima criminalității cibernetice

2

- evalueze riscul de (re) victimizare și victimizare a criminalității cibernetice, în general
- stabilească măsuri de securitate cibernetică și comportamente personale de protecție online

3

- identifice nevoile victimei criminalității cibernetice
- activeze resurse și servicii adecvate pentru a răspunde nevoilor victimei și pentru a aborda / minimiza impactul experienței de victimizare cibernetică

Colectarea informațiilor ar trebui să vizeze 3 domenii:

1. **Istoricul personal și pre-victimizare**
   Specialistul ar trebui să caute să colecteze informații despre contextul familial, profesional și social și ar trebui, de asemenea, să încerce să evalueze posibilele episoade de victimizare anterioare, precum și obiceiurile de utilizare a internetului, TIC și a rețelelor sociale, comportamentul / activitățile de risc, măsurile de securitate informatică adoptate sau nu precum și comportamentele personale de protecție online.

2. **Experiența victimizării informatice**
   În acest domeniu, ar trebui făcută o încercare de a aduna toate informațiile posibile despre situația criminalității informatice trăite de victimă, cu detalii despre circumstanțe, inclusiv: informații despre ceea ce s-a întâmplat; cum s-a întâmplat; ce instrumente de comunicare sprijinite de TIC și / sau Internet au fost utilizate; cu cine au fost dezvăluite / partajate dovezi ale criminalității informatice și / sau prin care platforme; cine sunt făptașii și care este relația dintre victimă și făptași; când a început situația de victimizare informatică și dacă este în curs; dacă există sau nu o coincidență între victimizarea informatică și alte forme de victimizare tradițională care implică aceiași făptași sau alții; ce măsuri au fost deja luate de victimă.

3. **Istoricul post-victimizare**
   Obiectivul este de a analiza și evalua impactul victimizării informatice, înțelegând consecințele, mecanismele de coping puse în aplicare, factorii de protecție disponibili victimei, alături de evaluarea sprijinului familial și social și a capacității victimei de a gestiona impactul și de a-și recăpăta controlul asupra vieții lor. De asemenea, este important să se evalueze motivația victimei pentru adoptarea măsurilor preventive și stabilirea unui plan de protecție.

2.4. Cazul specific al copiilor și tinerilor victime ale criminalității informatice

După cum s-a abordat în partea I a acestui manual[69], copiii și tinerii constituie un grup vulnerabil la victimizarea informatică datorită obiceiurilor și comportamentelor lor în utilizarea internetului și a TIC, precum și a dificultății adulților în supravegherea acestor comportamente (în special în contextul familial).

Contactarea și sprijinirea copiilor și tinerilor victime ale criminalității informatice ar trebui:

1. Să fie întotdeauna ghidat de **promovarea și protecția drepturilor lor**;
1. Să îndeplinească caracteristicile și **etapele de dezvoltare** ale copilului sau tânărului;
1. Să ia în considerare, ori de câte ori este posibil, i**mplicarea familiei**;
2. Să se concentreze asupra educării pentru o utilizare sigură și conștientă a TIC și a internetului ca comportament de protecție împotriva revictimizării.

În cele ce urmează, vom examina mai detaliat fiecare dintre aceste puncte.

1

- **promovarea și protejarea drepturilor copiilor pe tot parcursul sprijinului acordat unui copil / adult tânăr victimă a criminalității cibernetice**

Atunci când contactați și sprijiniți copiii și tinerii care sunt victime ale infracțiunilor în general și ale criminalității informatice în special, acțiunile specialiștilor ar trebui să protejeze întotdeauna drepturile copiilor și tinerilor. Acest manual nu intenționează să examineze această chestiune în mod cuprinzător și, ținând seama de particularitățile legislației naționale din fiecare stat membru, putem, în termeni generali, să spunem că fiecare specialist care contactează sau susține un copil sau o victimă tânără ar trebui să cunoască legislația în vigoare[70] și să-și definească acțiunile în consecință.

Convenția privind drepturile copilului[71], care include un set de drepturi universale de bază la care ar trebui să aibă acces toți copiii, conține câteva principii fundamentale care sunt adecvate oricărei intervenții cu copiii și tinerii. Acestea sunt:

- **Interesul superior al copilului**, care afirmă pe scurt că toate legile și acțiunile care afectează copiii ar trebui să pună interesele copilului pe primul loc, favorizându-i în cel mai bun mod posibil.
- **Nediscriminarea**, principiul conform căruia niciun copil nu ar trebui să fie dezavantajat (sau avantajat) din cauza rasei, culorii, sexului, limbii, religiei, naționalității, originii etnice sau sociale, opiniei politice sau de altă natură, statutului economic sau stării fizice sau mentale.

[69] Consultați Partea I, secțiunea 3.2 a acestui manual.

[70] În cazul Portugaliei, Legea nr. 147/99, din 1 septembrie, privind protecția copiilor și tinerilor în pericol și modificările ulterioare, vizează promovarea drepturilor și protecției copiilor și tinerilor aflați în pericol, pentru a le asigura bunăstarea și dezvoltarea deplină. Consultați legislația disponibilă la https://apav.pt/apav_v3/images/pdf/proteccao_criancas_jovens_perigo.pdf

[71] Consultați textul integral la: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

- **Supraviețuirea, dezvoltarea și protecția**, conform cărora autoritățile ar trebui să protejeze toți copiii și să contribuie la asigurarea deplinei lor dezvoltări fizice, sociale, spirituale și morale.
- **Participarea**, conform căreia toți copiii au dreptul de a avea un cuvânt de spus în deciziile care îi afectează, precum și de a fi audiați în problemele care îi privesc.

Prin urmare, specialiștii și organizația lor de sprijin ar trebui să stabilească, să definească și să pună în aplicare intervenția lor în conformitate cu aceste principii și cu legislația relevantă, ținând seama întotdeauna de necesitatea promovării **exercitării depline a drepturilor copiilor și tinerilor**.

2

- **respectați și țineți cont de etapele de dezvoltare ale copilului sau tânărului în timpul procesului de sprijin**

Contactarea și furnizarea de asistență pentru un copil sau o persoană tânără victimă a criminalității informatice trebuie să fie neapărat distinctă de cea oferită unui adult victimă a criminalității informatice.

Specialiștii ar trebui să cunoască principalele etape **în procesul de dezvoltare al copiilor sau tinerilor**, în special în ceea ce privește limbajul și comunicarea și să își adapteze strategiile de comunicare în consecință pe parcursul activității lor (APAV, 2019).

Tabelul următor rezumă, în termeni generici, principalele etape în procesul general de dezvoltare a unui copil sau a unei persoane tinere, în funcție de grupa de vârstă.

Tabel 4: Etapele cheie în procesul de dezvoltare a unui copil / tânăr

	Desenvolvimento físico	Dezvoltarea emoțională și cognitivă (inclusiv limbajul)	Dezvoltarea socială și morală
3-6 ani	• Poate desena și face alte activități manuale • Își poate scrie propriul nume • Corpul se dezvoltă, luând formele corpului adult • Dexteritatea și abilitățile de coordonare cresc	• Își amintește de experiențele familiare • Folosește un anumit vocabular • Poate ajusta vorbirea în funcție de caracteristicile interlocutorului (cum ar fi vârsta, sexul și statutul social)	• Poate interpreta, prezice și influența reacțiile altor persoane • Stabilește primele prietenii • Apar emoții conștiente de sine (cum ar fi rușinea și vinovăția) • Are un control relativ asupra propriilor emoții
6-12 anI	• Creșterea progresivă a greutății și înălțimii • Scrierea de mână devine mai mică și mai lizibilă • Desenele sunt mai structurate • Jocurile și glumele care implică alergarea, emoția și competiția sunt obișnuite • Capacitatea de răspuns rapid este dezvoltată la nivelul dexterității motrice • Indicatorii pubertății pot fi evidenți, în special în cazul fetelor	• Gândurile și durata atenției sunt mai concentrate • Raționament inductiv • Poate lega experiențele de evenimente specifice • Creșterea vocabularului	• Devine mai independent și mai responsabil • Distinge între a avea succes și a nu avea succes • Este conștient de propriile eforturi vs șansă / noroc în obținerea unui rezultat dat • Se poate pune în locul celuilalt (empatie)
12-18 anI	• Pubertate • Menstruația și țesutul adipos cresc la fete • Se schimbă vocea și există o creștere a masei musculare, în cazul băieților • Interes mai mare pentru sexualitate	• Poate discuta eficient • Mai conștient(ă) de sine și mai concentrat(ă) • Dezvoltarea raționamentului ipotetic-deductiv • Poate face ajustări subtile în vorbire • Poate face planuri și poate lua decizii	• Conflict sporit cu părinții / familia • Apropierea față de grupurile de colegi și apariția unor situații de presiune a colegilor • Căutarea propriei identități • Dezvoltarea relațiilor intime

Tabelul următor prezintă câteva dintre principalele diferențe în abordarea și comunicarea cu copiii și tinerii din diferite grupe de vârstă, care trebuie luate în considerare de către specialist în procesul lor de contact și sprijin (APAV, 2011).

Quadro II-5: Abordagem e comunicação com crianças e jovens de diferentes faixas etárias

	1-6 ani	6-12 ani	12-18 ani
Cum vă prezentați	Fundamental îndreptată către copil. Copilul este încă prea mic pentru a înțelege informațiile furnizate.	Copilul arată mai mult interes pentru informațiile furnizate și o capacitate mai mare de a le înțelege.	Copilul / tânărul înțelege informațiile furnizate, dar poate arăta reticența de a participa la un program de intervenție sau la un proces de susținere a victimelor.
Descrierea evenimentului	Exprimat de preferință prin desene sau jocuri, mai degrabă decât prin expresie verbală.	Capabil să comunice mai multe detalii decât copiii mai mici. Copiii mai mari preferă să se exprime verbal, uneori refuzând să folosească desene și jocuri.	Descrierea evenimentului este detaliată. Există sentimente de vinovăție de sine.
Psihoeducația	Se adresează fundamental familiei / părinților. Copilul va asimila informații simple, cum ar fi recunoașterea situației și poate simula un mod de a face față acesteia.	Destinat copilului, integrând familia / părinții în procesul de psihoeducare.	Direcționat către / prin copil

În plus, este important ca specialiștii, atunci când contactează sau susțin copiii sau tinerii victime ale criminalității informatice, să creeze toate condițiile, și anume prin **modul în care comunică cu copiii / tinerii**, pentru a-i împiedica să trăiască situația ca un fel de „interogatoriu al poliției". Aceasta nu este cu siguranță intenția și este important să avem un mediu confortabil și informal, care să contribuie la stabilirea unei relații de încredere între specialiști și copiii / tinerii victime.

În cazul copiilor mai mici, sprijinul poate necesita prezența unei rude sau a unui reprezentant legal până când copilul se obișnuiește cu specialistul și se simte în siguranță fără ruda sau reprezentantul legal (APAV, 2019).

- **Implicati familia ori de câte ori este posibil**

3

Rolul familiei și al părinților este crucial în situațiile de criminalitate informatică care vizează copiii și tinerii. Aceștia au un rol preventiv, prin informarea, supravegherea și, după caz, restricționarea

utilizării internetului și TIC de către copii și tineri (Öztürk & Akcan, 2016). **Implicarea familiei în situații în care criminalitatea informatică a avut deja loc este la fel de importantă** din moment ce:

- au un rol important în informarea despre povestea de viață a copilului sau a tânărului;
- participarea / frecvența implicării copilului sau tânărului victimă în procesul de sprijin depinde în mare măsură de disponibilitatea și deschiderea spre cooperare a familiei / părinților;
- sunt, de asemenea, elemente cheie pentru psiho-educația copiilor sau tinerilor și prevenirea revictimizării.

Specialiștii ar trebui să înțeleagă în ce măsură conștientizarea experienței de victimizare informatică a copiilor / tinerilor a contribuit la schimbări în funcționarea personală, maritală și familială. **Abordarea impactului și consecințelor experienței de victimizare informatică asupra familiei va contribui, de asemenea, la recuperarea copilului**. Reacțiile familiei la experiența victimizării informatice a copiilor și tinerilor sunt similare din toate punctele de vedere cu reacțiile la situațiile de violență și infracțiuni *tradiționale* (APAV, 2011):

- **Dorința de răzbunare**. O reacție comună, asociată cu un sentiment de revoltă, este dorința de răzbunare, de a lua „dreptatea în propriile lor mâini";
- **Sentimentul de vinovăție**. Familia se poate simți vinovată pentru că nu a descoperit / suspectat că copilul sau tânărul a fost supus infracțiunilor sau violenței;
- **„Subiect dur"**. Discuția cu copilul sau tânărul despre violența căreia i-a fost victimă este de obicei o provocare foarte dificilă pentru familie și părinți. Chiar și așa, acest dialog este important pentru a stabili o mai mare încredere în relația dintre familie și copil sau tânăr. Cu toate acestea, familia poate încerca, de asemenea, să facă presiuni asupra copilului sau tânărului pentru a vorbi despre situația de victimizare, care se pot dovedi contraproductive;
- **Schimbarea relațională**. Relația cu copilul sau tânărul se poate de asemenea schimba: relația *familie / părinte-copil / tânăr victimă* poate deveni mai dificilă și tulbure de jenă și sentimente reciproce de vinovăție și rușine;
- **Neîncredere în intervenție**. În multe cazuri, familia poate exprima lipsa de încredere în instituții, în special în autoritățile de poliție. Faptul că nu li se oferă informații cu privire la investigațiile în curs este un factor cheie;
- **Impactul general asupra vieții**. Toate domeniile vieții personale, familiale, sociale și profesionale ale membrilor familiei și ale părinților pot fi afectate;
- **Nevoia de sprijin**. În plus față de sprijinul și munca cu copiii sau tinerii care sunt victime ale criminalității informatice, familia și părinții pot avea nevoie de sprijin specific pentru a-i ajuta cât mai mult în sarcinile și provocările indicate mai sus.

4

- **Psihoeducație pentru o utilizare sigură și conștientă a TIC și a internetului**

Acțiunile specialiștilor și ale organizației lor în situații de victimizare informatică a copiilor și tinerilor ar trebui, de asemenea, să fie preocupați, pe lângă a răspunde la nevoile apărute prin experiența criminalității informatice, cu **promovarea comportamentelor sigure și conștiente atunci când se utilizează internetul și TIC** - scopul este de a preveni implicarea copiilor sau tinerilor în noi situații de risc sau situații de victimizare informatică repetată.

Este important să vă asigurați că copiii și tinerii victime sunt educați în ceea ce privește utilizarea sigură și adecvată a internetului și a TIC, care include, de exemplu: adoptarea unor comportamente online adecvate pentru protecția personală; utilizarea pozitivă și sigură a TIC și a internetului; implementarea mecanismelor de securitate informatică în instrumentele TIC și de comunicare folosite de internet; identificarea situațiilor de risc de victimizare informatică și acționarea adecvată (Martellozzo & Jane, 2017; Wolak, Finkelhor, Mitchell & Ybarra, 2010; Lwin, Ang & Liu, 2013; Wright, 2015).

IMPORTANT | PRACTICA ÎN FOCUS:

În Marea Britanie, programul *ThinkUKnow* oferă informații adaptate copiilor de diferite vârste, precum și familiilor, părinților, tutorilor legali și educatorilor despre criminalitatea informatică și siguranța online.

Acest program, creat de *Centrul de Exploatare și Protecție Online a Copilului (CEOP)*, oferă sfaturi și informații privind siguranța cu privire la o serie de aspecte legate de utilizarea internetului și a TIC și a situațiilor de risc rezultate (Marczak & Coyne, 2010).

Platforma este disponibilă la: www.thinkuknow.co.uk/

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

În acest capitol al manualului și în strânsă legătură cu liniile directoare generale pentru contact, comunicare și colectare de informații discutate în capitolul anterior, ne vom concentra pe sprijin și intervenție pentru victimele criminalității informatice.

Ținând cont de consecințele experienței de victimizare informatică și de nevoile de sprijin care au fost examinate în capitolul 4 din Partea I a acestui manual, ne vom concentra pe sprijinul emoțional, intervenția în situații de criză și aspectele centrale ale sprijinului de specialitate pentru victimele criminalității informatice.

Având în vedere gama largă de forme de criminalitate informatică, este important să subliniem că conținutul prezentat aici nu este considerat singurul răspuns posibil care trebuie pus în aplicare cu orice victimă a criminalității informatice. Dimpotrivă, acesta constituie o foaie de parcurs largă, având în vedere orientări de acțiune care pot ajuta profesioniștii și organizațiile să ajusteze configurarea și livrarea intervențiilor lor în funcție de propriile caracteristici și obiective și care vizează să ofere cel mai bun răspuns posibil la nevoile victimelor criminalității informatice.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Întrucât acest capitol și cele anterioare din partea de intervenție a acestui manual presupun că sprijinul pentru victimele criminalității informatice este furnizat de organizații, și anume organizațiile de sprijinire a victimelor, unele **cerințe de bază și aspecte practice pentru dezvoltarea și funcționarea serviciilor de sprijin pentru victimele criminalității informatice** trebuie să fie adresate.

Orice organizație care intenționează să dezvolte și să implementeze un serviciu de asistență sau un răspuns destinat victimelor criminalității informatice ar trebui să ia în considerare în primul rând efectuarea unei **evaluări diagnostice a capacităților sale organizaționale**[72].

Unele dintre domeniile pe care organizația ar trebui să le analizeze intern sunt:

- Adecvarea acestui serviciu sau răspuns de sprijin la misiunea și activitățile organizației în sine și, atunci când este cazul, niveluri de integrare cu celelalte servicii ale acestora (cum ar fi servicii și răspunsuri de sprijin pentru victimele infracțiunilor și violenței);
- Capacitatea financiară de a stimula dezvoltarea serviciului de sprijin sau a răspunsului și funcționarea acestuia, având în vedere în special existența sau nu a resurselor proprii, accesul la finanțare externă și / sau sponsorizare;
- Accesul la resursele materiale, tehnologice și logistice necesare dezvoltării și operării serviciului sau a răspunsului de sprijin;
- Cunoștințe organizaționale despre sprijinul care trebuie oferit și despre criminalitatea informatică, inclusiv diferitele tipuri de criminalitate informatică, factorii de risc și impactul victimizării informatice și cadrul legal aplicabil;
- Capacitatea tehnică organizațională de a dezvolta proceduri pentru serviciul sau răspunsul de sprijin pe care intenționează să îl opereze, luând în considerare adecvarea sa în lumina misiunii, principiilor și valorilor organizației, a celorlalte forme de sprijin / servicii pe care le oferă și a legislației aplicabile;
- Parteneriatele actuale (formale / informale) cu alte organizații cu experiență și expertiză în acest domeniu și posibilitatea participării / dezvoltării acțiunilor care permit schimbul / obținerea de

[72] Adaptare după Safety Net Project - https://www.techsafety.org/resources-agencyuse.

cunoștințe, experiențe și bune practici;
- Resursele umane existente (remunerate și / sau voluntari) calificate să ofere acest tip de sprijin și capacitate tehnică și financiară pentru pregătirea și calificarea acestora.

Astfel, pe scurt, **pregătirea organizației pentru implementarea** unui serviciu de răspuns sau de sprijin pentru victimele criminalității informatice va include următorii pași de bază:

1. Definiți obiectivele serviciului de răspuns sau de asistență dorit. Unele dintre obiective pot fi, de exemplu: informare / conștientizare; suport emoțional; suport practic; asistență sau sfaturi mai specifice la un anumit nivel (de exemplu, informații juridice); trimiterea către alte servicii / răspunsuri / organizații adecvate pentru a face față situației.
2. Identificați destinatarii serviciului de răspuns sau de sprijin: scopul poate fi implementarea unui serviciu de răspuns sau de sprijin și / sau informații pentru victimele oricărei forme de criminalitate informatică; sau poate viza grupuri specifice de victime și / sau forme specifice de criminalitate informatică. Un exemplu îl reprezintă căile de raportare a materialelor de abuz sau exploatare sexuală asupra copiilor.
3. 3. Stabiliți proceduri și strategii de articulare și integrare cu răspunsurile celeilalte organizații și servicii de sprijin pentru victimele infracțiunilor, dacă sunt disponibile, definind cum și în ce mod vor fi tratate intern informațiile despre o anumită situație de victimizare informatică, dacă este necesar, pentru o mai bună abordare a nevoilor victimei. Ar trebui luate în considerare și legăturile externe și cooperarea interinstituțională[73].
4. 4. Elaborați proceduri specifice pentru sprijinul care trebuie furnizat, luând în considerare obiectivele și destinatarii serviciului de răspuns sau de sprijin și legislația aplicabilă și codurile de conduită profesionale, atunci când este cazul. În plus, organizația ar trebui să aibă, de asemenea, o înțelegere largă a fenomenului, a impactului său asupra victimelor și a nevoilor declanșate de experiențele de victimizare informatică[74].
5. Selectați și instruiți resursele umane pentru funcționarea serviciului de răspuns sau de asistență[75].
6. Diseminați și faceți publicitate serviciului de răspuns sau de asistență[76].

3.1. De la sprijinul emoțional la intervenția în criză

Pe scurt, sprijinul emoțional pentru o victimă a criminalității informatice se bazează în mare măsură pe poziționarea și atitudinea profesionistului cu privire la dimensiunile deja discutate în acest manual și enumerate mai jos:

- **Comunicarea empatică**, care include ascultarea activă;
- **Limbaj non-verbal** care demonstrează disponibilitate, deschidere și consecvență cu ascultarea activă;
- **Recunoașterea plângerii și respectarea ritmului victimei** atunci când împărtășesc;
- Promovarea **expresiei emoționale a victimei și validarea experienței**, reacțiilor, emoțiilor / sentimentelor, comportamentelor, gândurilor și semnificațiilor atribuite acelei experiențe.

În acest context, subliniem din nou că **acest sprijin emoțional este deosebit de important atunci când se colectează informații** de la victimele infracțiunilor despre experiența lor de victimizare informatică

[73] Consultați secțiunile 3.5.1.3. și 3.5.3.2. din Capitolul 3 al Părții II ale acestui manual pentru mai multe informații privind lucrul în colaborare.

[74] Consultați capitolele 1, 3 și 4 din partea I a acestui manual pentru informații cuprinzătoare despre fenomenul criminalității informatice, teoriile explicative, factorii de risc asociați criminalității informatice și impactul acesteia.

[75] Consultați partea II, capitolul 1 al acestui manual pentru informații despre abilitățile personale și tehnice ale profesionistului pentru sprijinirea victimelor criminalității informatice.

[76] Consultați partea II, secțiunea 4.2 din acest manual pentru informații despre rolul campaniilor de informare publică și de sensibilizare în diseminarea informațiilor privind resursele existente pentru sprijinirea și protejarea victimelor criminalității informatice.

(nu în ultimul rând pentru că colectarea de informații, cu necesitatea ulterioară de a împărtăși informații despre experiența victimizării informatice, poate declanșa amintiri și sentimente negative despre experiența criminalității informatice; în plus, colectarea de informații este în sine un moment incomod și vulnerabil pentru victimă). Prin urmare, acest sprijin emoțional rămâne important pe tot parcursul intervenției cu victima criminalității informatice, indiferent de durata mai mică sau mai lungă a intervenției.

Cu toate acestea, în anumite circumstanțe, victima criminalității informatice poate solicita sprijinul specialistului și a organizației acestuia (și anume organizațiile de sprijinire a victimelor) într-o **situație de criză**.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Experiența victimizării informatice, prin caracterul potențial neobișnuit și neprevăzut și amenințarea (reală sau percepută) pentru integritatea fizică și / sau psihologică a victimei, poate duce la o **situație de criză** (APAV, 2013b).

Situația de criză este observabilă prin următoarele manifestări:

- **Reacții psihologice intense**, precum plâns, panică, confuzie, angoasă, rușine, stima de sine scăzută, vinovăție, furie, tulburări psihosomatice și predominarea amintirilor despre eveniment;
- **Presiuni sociale și economice** care conduc la blocaje emoționale sau psihologice, asociate cu **necunoașterea drepturilor lor**.

Durata și intensitatea situației de criză depind de gradul de violență împotriva victimei, de resursele interne ale acestora pentru a face față problemei și de resursele externe de care dispun, inclusiv sprijinul (informal și formal) primit după situația de victimizare.

Intervenția în criză (sau primul ajutor psihologic) este, prin urmare, o acțiune intensivă, concentrată și limitată în timp, orientată spre rezolvarea problemelor actuale și pentru a răspunde unor obiective specifice. Este un răspuns care oferă sprijin inițial și îngrijire practică, ne-invazivă, în situații de criză sau de urgență.

Sarcina inițială a specialistului care contactează o victimă a criminalității informatice într-o situație de criză este, prin urmare, legată de:

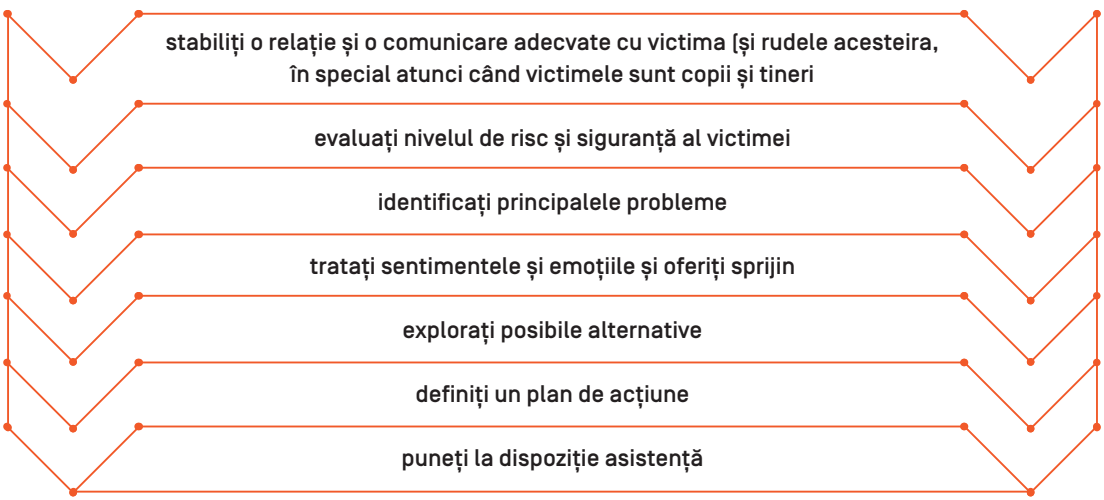
- **Evaluarea siguranței victimei** și a **capacității de auto-îngrijire** în situații potențial traumatice, considerând că resursele personale și sociale de care dispune pot fi insuficiente pentru a răspunde în mod adecvat unei situații extrem de solicitante.
- Operaționalizarea sarcinilor de intervenție care vizează **recuperarea și reorganizarea victimei**, reducând impactul negativ al victimizării informatice și asigurând siguranța și bunăstarea lor fizică și psihologică.

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

Intervenția în caz de criză ar trebui să urmărească să răspundă la următoarele obiective, similare cu liniile directoare generale pentru sprijinirea victimelor criminalității informatice (consultați Tabelul 2):

- Demontați ideea de „vulnerabilitate unică";
- Adresați căutarea explicațiilor;
- Adresați sentimentele de vinovăție ale victimei;
- Evitați reducerea la tăcere sau presiunea de „a uita";
- Promovați speranța în recuperarea și soluționarea problemei;
- Explicați procedurile legale necesare.

Prin urmare, intervenția în caz de criză ar trebui să se bazeze pe următorii **pași**:



În acest tip de intervenție, am sugerat adoptarea următoarelor strategii, fără a aduce atingere altora care ar putea fi considerate adecvate (APAV, 2013b):

Stabiliți un raport cu victima:
Specialistul ar trebui să încerce să stabilească o relație de încredere cu victima, identificând evenimentele care au condus la căutarea de sprijin, care să permită identificarea problemelor cheie.

Evaluați:
Specialiștii ar trebui să fie conștienți de sănătatea mintală a victimei, dacă există gânduri suicidare, cu cât de multă anxietate, agitație și suferință se confruntă și, în special, dacă situația lor mentală le permite să răspundă în mod adecvat obligațiilor practice care decurg din victimizarea informatică.

De asemenea, specialistul ar trebui să evalueze riscul (detalii suplimentare vor fi acoperite în următoarele secțiuni ale acestui manual), precum și existența și calitatea asistenței oferite de rețeaua de asistență principală (familie și / sau prieteni).

Reduceți stresul și angoasa:
Este obișnuit ca victima să se regăsească într-o situație de stres și angoasă. Comunicarea cu victima într-un mod sigur și liniștitor este o strategie adecvată pentru a reduce aceste simptome. În mod similar, atunci când contactează victima, specialistul ar trebui să explice că aceste reacții sunt normale, legitime și pot apărea în fața unor experiențe personale negative, provocatoare și / sau solicitante.

În acest proces, specialistul ar trebui să comunice în mod natural cu victima (fără a neglija gravitatea situației trăite), acordându-i atenție și fără a întări comportamentul agitat sau afectat emoțional.

Arătați interes și motivați victima:
Specialistul ar trebui să manifeste interes, dorință de a asculta și de a înțelege victima și situația acesteia (consultați secțiunea 2.2 despre empatie din această parte a Manualului). De asemenea, ar trebui să stimuleze speranța într-o rezoluție pozitivă (deși realistă) a situației, care va promova încrederea în sine a victimei.

De asemenea, este important să încurajați victima să își găsească propriile strategii pentru a depăși experiența victimizării informatice prin consolidarea capacităților sale.

Clarificați:
Este important să se clarifice căror cerințe va trebui să răspundă victima ca urmare a criminalității informatice suferite, inclusiv obligații practice, cum ar fi legătura cu băncile în situații de criminalitate informatică motivate financiar, de exemplu, sau legătura cu platformele unde este disponibil conținut ilegal pentru a solicita îndepărtarea acestuia.

Informați și validați drepturile victimei:
Specialistul ar trebui să ofere victimei informații cu privire la drepturile sale, cu privire la funcționarea sistemului de justiție și cu privire la avantajele și dezavantajele raportării infracțiunii, contribuind astfel la o decizie informată a victimei în această privință. Unul dintre avantajele care pot fi asociate cu decizia de raportare poate fi asigurarea victimei că a adoptat o atitudine activă față de infracțiunea suferită. Un alt avantaj pe care specialistul îl poate evidenția este că, raportând situația lor specifică, victima contribuie la prevenire și permite altor persoane să fie „scutite" de a experimenta situații de victimizare informatică similare. Dezavantajele sunt legate de dificultățile cu care se poate confrunta victima pe tot parcursul procesului judiciar, și anume posibilele obstacole în cercetarea penală și propriile dificultăți emoționale, precum rușinea și nevoia de a retrăi evenimentul traumatic de fiecare dată când li se cere să raporteze faptele.

Specialistul ar trebui să alerteze victima cu privire la necesitatea de a păstra dovezile infracțiunii

dacă are acces la acestea (cum ar fi, de exemplu, link-uri unde este posibil să se acceseze informații despre actele de agresiune online la care a fost supusă, precum și mesaje, videoclipuri și / sau alte fișiere pe care le-a primit în timpul victimizării informatice sau chiar tipărituri / copii care au în vedere publicitatea / difuzarea online a agresiunii).

Trimiterea către autoritățile judiciare și de poliție:
Dacă victima nu a contactat încă autoritățile judiciare și de poliție pentru investigarea acestor infracțiuni până când contactează specialistul în asistență, atunci specialistul poate, cu acordul victimei, să faciliteze o astfel de sesizare. În acest scop, este important ca organizația specialistului să definească și / sau să caute să implementeze mecanisme care să faciliteze cooperarea interinstituțională, pe care le vom aborda și în acest manual (consultați secțiunile 3.5.1.3. și 3.5.3.2. din acest capitol, partea II din acest manual).

Asigurați suport:
Specialistul ar trebui să pună la dispoziția victimei serviciile de sprijin și răspunsurile disponibile prin intermediul organizației lor, care pot include, de exemplu, trimiterea la servicii de sprijin mai specifice furnizate de organizația lor și chiar resurse externe disponibile, la nivel local, regional sau național, prin intermediul articulării și cooperării interinstituționale.

IMPORTANT | PRACTICA ÎN FOCUS:

APAV coordonează, în Portugalia, o rețea specializată în sprijinirea copiilor și tinerilor victime ale violenței sexuale, numită Rețeaua CARE, care oferă sprijin psihologic, social și legal copiilor și tinerilor victime ale violenței sexuale, dar și rudelor și prietenilor.

Această Rețea are profesioniști specializați, distribuiți pe teritoriul național, care caută să asigure un serviciu descentralizat de calitate. Prin furnizarea de servicii itinerante, specialiștii ai Rețelei CARE vin în sprijinul victimelor și garantează copiilor și tinerilor victime, familiilor și prietenilor accesul la sprijin multidisciplinar, adaptat nevoilor identificate și în apropierea zonelor lor de reședință.

Astfel, atunci când o situație de violență sexuală împotriva copiilor și tinerilor este identificată în orice serviciu de asistență APAV - cum ar fi un birou de asistență pentru victime sau sistemul integrat de asistență la distanță / Linia de sprijin pentru victime | 116 006 -, există o trimitere (internă) a cazului către sprijin specializat de către Rețeaua CARE.

Informații suplimentare despre funcționarea rețelei CARE a APAV sunt disponibile la adresa www.apav.pt/care.

Informações adicionais sobre o funcionamento da Rede CARE da APAV estão disponíveis em www.apav.pt/care.

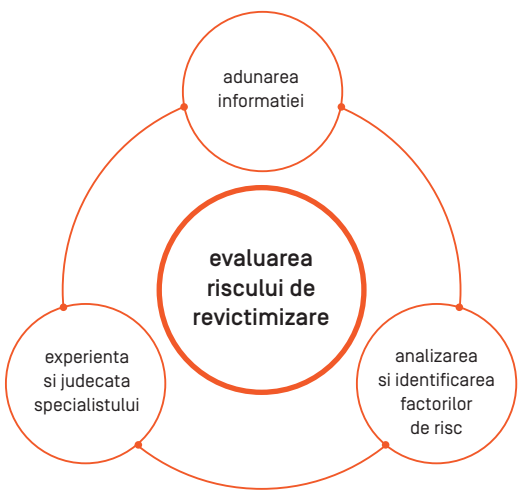
În urma intervenției de criză, poate fi necesară continuarea intervenției cu victima criminalității informatice pentru a promova recuperarea acesteia și a răspunde în mod adecvat nevoilor sale. În conformitate cu răspunsurile de sprijin oferite de alte organizații de sprijinire a victimelor altor forme

de victimizare, acest manual va aborda, de asemenea, aspectele centrale asociate intervenției juridice, psihologice și sociale specializate, iar aceste domenii vor fi, de asemenea, în conformitate cu nevoile identificate de obicei de către victimele infracțiunilor. Aspectele cheie ale intervenției specializate vor fi discutate în secțiunea 3.5 a acestui capitol.

3.2. Evaluarea riscului de revictimizare

Evaluarea gradului de risc al revictimizării evaluează probabilitatea unei noi victimizări informatice împotriva victimei. După colectarea informațiilor (consultați capitolul 2 din această parte a manualului), specialistul ar trebui să evalueze factorii de risc și protecție[77] ai victimei evidențiați în timpul intervenției, astfel încât nevoile de sprijin și intervenție să poată fi identificate.

Procesul de evaluare a riscului revictimizării rezultă astfel din convergența dintre informațiile împărtășite de victimă cu privire la experiența sa de victimizare informatică și utilizarea acestor informații pentru a identifica (într-un mod mai mult sau mai puțin structurat) factorii de risc de revictimizare (și cărora li se va acorda o atenție deosebită în planificarea intervenției și comportamentele personale de protecție online și măsurile de securitate informatică pentru a preveni revictimizarea). Experiența și judecata specialiștilor de sprijin este de asemenea importantă în acest proces de evaluare a riscurilor.

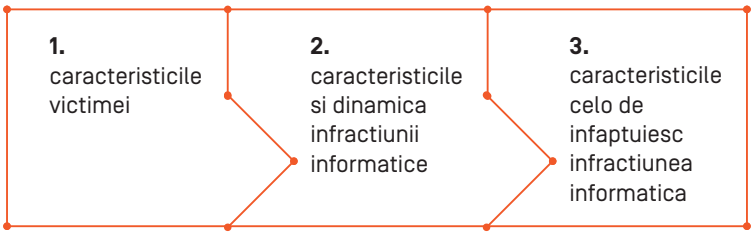


După cum s-a menționat în capitolul 3 al părții I a acestui manual, cercetarea privind factorii de risc asociați cu victimizarea informatică nu este, până în prezent, deosebit de extinsă și, deși pot fi identificați în continuare alți factori sau variabile, factori individuali legați de comportamentul victimei, în special intensitatea și obiceiurile de utilizare a internetului și a TIC și tipul de activități desfășurate

[77] Pentru informații suplimentare despre factorii de risc asociați cu hărțuirea informatică, vă rugăm să consultați partea I, capitolul 3 al acestui manual.

online, au fost asociate cu o vulnerabilitate crescută la criminalitatea informatică și cu riscul victimizării informatice (Wilsem, 2013; Brown și colab., 2017; van der Wagen & Pieters, 2018). Pe de altă parte, multiplicitatea formelor de criminalitate informatică face dificilă identificarea unui grup de factori de risc sau variabile care se aplică fără echivoc oricărui tip de criminalitate informatică.

Chiar și așa, doar în termeni generali, putem spune că evaluarea riscului de revictimizare ar trebui să se concentreze pe trei domenii de risc:



Cu toate acestea, și făcând aluzie din nou la natura multiplă a criminalității informatice, este clar că, de exemplu, **analiza riscului de revictimizare cauzată de infracțiunile informatice împotriva computerelor și sistemelor informatice** (infracțiuni informatice dependente)[78] are dificultăți în colectarea informațiilor care permit această lectură tripartită (pe baza caracteristicilor victimei, a dinamicii criminalității informatice și a caracteristicilor făptuitorului). De exemplu, în aceste cazuri făptuitorul acționează anonim și este foarte dificil să se identifice identitatea lor reală, astfel încât analiza caracteristicilor lor și contribuția lor la creșterea / reducerea riscului de revictimizare este, prin urmare, afectată negativ.

Pe de altă parte, identificarea și analiza riscurilor la trei niveluri sunt mai utile pentru a determina vulnerabilitatea victimei la **revictimizare în cazurile de criminalitate informatică facilitate sau practicate prin intermediul computerelor și sistemelor de informații**[79], în special în situațiile în care există o legătură relațională (online și / sau offline) între victimă și făptaș, deoarece aceste cazuri corespund mai ușor unei transpuneri a infracțiunilor *tradiționale* în spațiul informatic.

Tabelul următor prezintă câteva variabile și factori de risc asociați cu fiecare dintre domeniile de risc de mai sus, care pot fi utilizate de către specialist pentru a evalua riscul victimei de revictimizare.

Cu toate acestea, ar trebui să rețineți că acestea sunt variabile orientative și generice și nu iau în considerare dinamica specifică asociată fiecărei situații particulare de victimizare informatică.

[78] Consultați partea I, capitolul 1 al acestui manual pentru informații detaliate despre această conceptualizare.

[79] Idem.

Tabel 6: Variabile propuse pentru evaluarea riscului de revictimizare al victimei criminalității informatice

Caracteristicile victimei	Caracteristicile criminalității informatice
Factorii de risc legați de caracteristicile socio-demografice și individuale ale victimei și factorii de risc asociați cu comportamentul de utilizare a internetului și TIC.	*Caracteristicile și dinamica criminalității informatice, inclusiv relația / conexiunea (online și / sau offline) între victimă și făptuitor, în special în situațiile de criminalitate informatică facilitată de internet și TIC.*
Vârstă *Au fost evidențiate niveluri diferențiate de risc de victimizare informatică la copii / tineri și la persoanele în vârstă; în primii, prin obiceiurile de utilizare intensivă a internetului și TIC și, în cei din urmă, prin lipsa de alfabetizare tehnologică.* **Gen** *Nu există o viziune convenită din cercetare și studiile de prevalență și această variabilă ar trebui interpretată cu prudență. Deși sexul feminin este asociat cu niveluri mai ridicate de victimizare în diferite infracțiuni informatice, acest lucru se poate datora unei raportări mai mari. În unele infracțiuni informatice, bărbații sunt, de asemenea, asociați cu forme mai severe și mai grave de agresiune.* **Alte variabile individuale asociate cu o vulnerabilitate mai mare la victimizare** **Prezența dificultăților / handicapului mental și / sau cognitiv** *Aceste caracteristici pot limita sau împiedica identificarea / recunoașterea victimizării informatice și / sau divulgarea / cererea de asistență în urma victimizării informatice, ceea ce crește riscul revictimizării.* **Limba primară** *În situațiile în care limba principală a victimei este diferită de limba în care poate avea loc sprijinul / raportarea criminalității informatice, riscul revictimizării este mai mare și este asociat cu o vulnerabilitate mai mare la excludere și izolare socială.* **Experiențe anterioare de victimizare** *Dacă victima a fost deja țința criminalității informatice în trecut, riscul de revictimizare poate fi mai mare, mai ales dacă factorii de expunere la criminalitatea informatică nu s-au schimbat.* **Fără sprijin informal (de exemplu, familie; prieteni; colegi de muncă)** *Izolarea socială, în special absența unor relații sociale mai strânse și mai semnificative, este un factor de risc pentru victimizare.* **Factorii de risc asociați cu comportamentul de utilizare a internetului și TIC** **Alfabetizare tehnologică** *Abilitățile și cunoștințele legate de internet și TIC par să reducă riscul de victimizare informatică. Absența / insuficiența lor, pe de altă parte, pare să crească acest risc.*	**Cunoașterea autorului criminalității informatice** *Riscul de revictimizare este mai mare în situațiile în care făptuitorul și victima se cunosc (online și / sau offline). În aceste cazuri, cunoașterea rutinelor zilnice ale victimei, atât online, cât și offline, este mai mare, ceea ce crește riscul revictimizării.* **Relația cu autorul criminalității informatice** *În situațiile în care victima și făptașul au avut un fel de relație offline (cum ar fi foști parteneri intimi, colegi de muncă, prieteni), riscul revictimizării este mai mare.* **Existența unui istoric de victimizare de către autorul criminalității informatice** *Existența unor experiențe anterioare de victimizare practicate de același făptuitor indică un risc de revictimizare. Unul dintre cei mai buni predictori ai comportamentului actual al făptuitorului este comportamentul lor din trecut.* **Severitatea și impactul criminalității informatice** *De exemplu, faptul că criminalitatea informatică poate declanșa simptome de suferință emoțională și psihologică (cum ar fi atacuri de panică, frică intensă, flashback-uri, coșmaruri, tristețe profundă sau alte simptome / semne), poate reduce capacitatea de a căuta sprijin în prezent / viitor situații de victimizare.* **Durata și escaladarea criminalității informatice** *Dacă victimizarea informatică persistă - așa cum se întâmplă în multe situații informatice, de exemplu - pe lângă probabilitatea ca o conduită ilicită să devină mai intruzivă și mai agresivă pentru victimă, aceasta întărește și comportamentul făptuitorului, crescând riscul pentru victimă.* **Frica de autorul criminalității informatice** *Percepția victimei asupra fricii față de făptuitor, în special în cazurile în care se cunosc, este un indicator foarte important, chiar dacă există situații în care subestimează riscul.* **Încercările anterioare (nereușite) de a rezolva situația** *În plus față de descurajarea victimei, acest eșec încurajează făptuitorul să practice noi acte împotriva victimei, crescând riscul.* **Raportarea / reclamația** *Raportarea este un moment de risc pentru victimă, dată fiind posibilitatea represaliilor / răzbunării de către făptuitor.*

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

Niveluri de utilizare a internetului și TIC
Persoanele cu niveluri mai ridicate de utilizare a internetului și a TIC (de exemplu, zilnic) prezintă un risc mai mare de victimizare informatică.

Tipul activităților efectuate online / conținut consumat de obicei
Ratele mai mari de dezinhibare în comportamentele și interacțiunile online, precum și comportamente mai nesigure (cum ar fi descărcarea fișierelor de origine necunoscută) sunt asociate cu o vulnerabilitate crescută la victimizarea informatică.

Caracteristicile autorului criminalității informatice

Caracteristicile personale și sociale ale făptuitorului criminalității informatice, comportamentul lor anterior și alți indicatori de pericol care pot indica un risc mai mare de revictimizare pentru victimă, în special în situațiile de criminalitate informatică făcute posibile sau facilitate de internet și TIC.

NOTĂ: În această analiză a riscurilor, pe lângă dificultățile asociate tipologiilor de criminalitate informatică menționate mai sus, informațiile împărtășite de victimă pot să nu fie suficiente pentru a evalua factorii prezentați mai jos.

Existența **problemelor de sănătate mintală și / sau a consumului de droguri** de către autorul criminalității informatice (cunoscut de victimă)

Existența / istoricul **problemelor cu sistemul de justiție** de către autorul criminalității informatice (cunoscut de victimă)

Încercări de a **contacta / aborda / intimida** victima după episodul care a motivat-o să caute sprijin

Dorința de răzbunare a făptuitorului, în special atunci când victima și făptuitorul au avut o relație intimă anterioară și criminalitatea informatică apare ca o formă de represalii pentru încheierea relației (de exemplu, divulgarea non-consensuală a imaginilor și videoclipurilor)

Interes special pentru criminalitatea informatică, de ex. motive financiare și / sau căutare de senzații tari.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Specialistul (și organizația în care lucrează) ar trebui să decidă și să definească modul de desfășurare a colectării informațiilor pentru evaluarea riscului de revictimizare. În general:

- Colectarea informațiilor poate fi efectuată indirect de către specialist, folosind informațiile împărtășite de victimă la contactarea organizației / specialistului;
- Evaluarea riscului de revictimizare poate fi realizată într-un mod mai structurat, punând întrebări concrete cu privire la fiecare dintre variabilele enumerate mai sus (sau altele considerate relevante) și / sau prin instrumente specifice.

De asemenea, este important să ne amintim că evaluarea riscului de revictimizare este utilă numai dacă este însoțită de măsuri pentru a ajuta victima să gestioneze și să facă față situației și riscului, pentru a-și îmbunătăți siguranța și a preveni revictimizarea.

Atunci când definesc parametrii și variabilele pentru a evalua riscul, organizația și / sau specialistul ar trebui să ia în considerare, de asemenea, dezvoltarea unei informații și a unui plan de protecție pentru victimă, luând în considerare variabilele de risc identificate. Planul de protecție reprezintă un set de strategii de prevenire a revictimizării, convenite și definite între victimă și specialist, care include măsuri de protecție și comportamente împotriva noilor situații de infracțiuni, precum și strategii și instrucțiuni practice pentru tratarea și acțiunea cu o altă eventuală reapariție a victimizării informatice.

Planul de protecție (Finn & Banach, 2000) poate include, în funcție de tipul de criminalitate informatică suferită de victimă:

- Adoptarea de măsuri de securitate informatică și comportamente de protecție personală pentru a preveni revictimizarea, cum ar fi: stocarea informațiilor importante în fișiere și directoare protejate prin parolă; criptarea celor mai importante date; evitarea conectării și / sau partajării informațiilor personale în public sau utilizarea rețelelor wi-fi deschise; schimbarea parolelor; actualizarea software-ului antivirus; modificarea setărilor de confidențialitate pe rețelele sociale;
- Identificarea semnelor unui risc de victimizare informatică, de exemplu: redirecționare constantă către pagini web ciudate / necunoscute; apariția de mesaje pop-up, imagini, sunete ciudate sau aplicații instalate fără consimțământ etc.;
- Informații practice despre cum și unde să obțineți ajutor într-o situație de victimizare.

3.3. Evaluarea și identificarea nevoilor de sprijin

În urma colectării de informații împreună cu victima și luând în considerare rezultatele evaluării riscului de revictimizare, este important ca specialistul să identifice nevoile de sprijin ale victimei criminalității informatice.

Unele aspecte care pot ajuta specialistul să identifice nevoile care trebuie abordate sunt:

- În ce măsură și în ce mod(uri) simte victima că a fost afectată de infracțiunea / criminalitatea informatică care o vizează?
- Cum afectează experiența victimizării informatice funcționarea și bunăstarea psihologică și emoțională a victimei?
- Cum afectează experiența victimizării informatice sănătatea fizică a victimei?
- Cum afectează experiența victimizării informatice funcționării relaționale, profesionale / sociale și sociale a victimei?
- Cum schimbă experiența victimizării informatice rutina și calitatea vieții victimei (bunăstare generală)?
- Cum afectează experiența victimizării informatice percepțiile personale ale siguranței și securității informatice (inclusiv frica de infracțiuni)?
- În ce măsură experiența victimizării informatice a afectat persoanele din rețeaua socială apropiată a victimei și care sunt aceste impacturi?
- Ce își dorește și trebuie să se întâmple victima după experiența de victimizare informatică?

În funcție de răspunsul la întrebările anterioare, specialistul, împreună cu victima, ar trebui să afle dacă:

- Este necesar să se ofere strategii pentru creșterea siguranței victimei pentru a face față posibilelor noi episoade de infracțiuni?

- Este necesar să recomandăm victimei să contacteze poliția / autoritățile judiciare?
- Este necesară să facem victima conștientă cu privire la necesitatea unui sprijin, informații și / sau intervenții mai specifice (de exemplu, juridice, medicale, psihologice sau altele)?
- Este necesar să fie motivată victima pentru a fi trimisă la alte servicii sau organizații (de exemplu, pentru sprijin medical / psihiatric specific).

IMPORTANT | PRACTICA ÎN FOCUS:

Ca parte a proiectului EVVI (*EValuarea VIctimelor*), promovat de Ministerul Justiției din Franța, au fost elaborate un chestionar individual de evaluare a nevoilor victimelor și un ghid practic.

Acest instrument de evaluare a nevoilor victimelor este structurat în diferite domenii:

- Caracteristicile individuale ale victimei și vulnerabilitatea personală, cum ar fi vârsta, sexul, etnia, prezența limitărilor fizice și / sau cognitive sau a dizabilităților, printre altele;
- Riscul și frica de infracțiune, inclusiv tipul și natura infracțiunii și circumstanțele acesteia;
- Evaluarea situației actuale a victimei;
- Istoricul victimizării și informații despre făptuitor.

Ghidul și instrumentul de evaluare sunt disponibile la adresa http://www.justice.gouv.fr/publication/evvi_guide_en.pdf .

Unele dintre **nevoile identificate** pot fi satisfăcute de organizația care sprijină victima criminalității informatice, prin serviciile și răspunsurile sale de sprijin.

Cu toate acestea, alte nevoi (de exemplu, asistență medicală și psihoterapeutică) pot necesita **cooperare interinstituțională și implicarea altor structuri**, de exemplu sistemul de justiție penală și alte sisteme. Mai mult, parteneriatele intersectoriale, inclusiv cele dintre stat și societatea civilă și organizațiile de voluntariat, par a fi importante pentru a răspunde mai bine nevoilor victimelor criminalității informatice, deoarece acestea contribuie la creșterea flexibilității și accesibilității acestor servicii și a răspunsurilor de sprijin (Wedlock & Tapley, 2016).

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Capacitatea organizației de a răspunde nevoilor victimei criminalității informatice va depinde de:

- competențele și misiunea organizației;
- existența / disponibilitatea serviciilor de sprijin sau a răspunsurilor oferite de organizație și la care specialistul poate trimite victima criminalității informatice pentru sprijin specific / specializat;
- existența serviciilor sau răspunsurilor comunitare de sprijin (de exemplu, sănătate, securitate socială, justiție și siguranță) și chiar posibile protocoale de cooperare interinstituțională[80].

[80] Consultați punctele 3.5.1.3. și 3.5.3.2. din acest capitol din partea II a manualului pentru informații privind cooperarea interinstituțională și networking.

3.4. Rolul sprijinului pe internet în sprijinirea victimelor criminalității informatice

Până în acest moment din acest manual, ne-am adresat contactului și asistenței cu victimele criminalității informatice, presupunând că acestea au loc prin modalități convenționale (adică față în față și chiar telefonic) de asistență, informare și intervenție. Cu toate acestea, la fel cum criminalitatea și violența au trecut barierele fizice și convenționale și au întruchipat apariția criminalității informatice și multiplele fenomene asociate acesteia, au evoluat, de asemenea, și contactul și sprijinul pentru victimele infracțiunilor.

Serviciile de asistență pe internet furnizate de organizațiile de sprijinire a victimelor pentru sprijinirea și informarea victimelor infracțiunilor devin din ce în ce mai frecvente.

În mod similar, sprijinul pentru victimele infracțiunilor informatice poate fi oferit și prin servicii de asistență convenționale (inclusiv asistență față în față și asistență telefonică), precum și prin servicii de asistență pe Internet, acestea din urmă considerate ca fiind canale la fel de valide pentru accesul la o mare varietate de servicii (Dooley și colab., 2010).

Prin urmare, este important să deconstruiți unele aspecte asociate asistenței prin Internet.

Asistența pe internet este o desemnare cuprinzătoare care se referă la întreg suportul, informațiile și / sau intervențiile obținute de la distanță prin Internet și TIC (Mallen, Vogel, Rochlen și Day, 2005, Barak, Klein și Proudfoot, 2009 cit în APAV, 2017) .

Această desemnare acoperă un set divers de metode, inclusiv mecanisme de intervenție sau de sprijin în cazul în care poate exista sau nu interacțiune între un utilizator și un profesionist. Diferitele metode de asistență prin Internet pot diferi în (in)existența interacțiunii cu un profesionist, dar și în modul utilizat pentru a comunica (de exemplu, audio, video și / sau text), modul în care acestea completează alte forme de intervenție / sprijin și modul în care se desfășoară comunicarea (sincronă sau nesincronă) (Robinson, 2009, Callahan & Inckle, 2012 cit in *idem*).

Există mai multe forme de asistență pe Internet, și anume: programe de intervenție / suport bazate pe internet; suport online; bloguri, forumuri online și grupuri de ajutor reciproc; software operat prin internet; alte forme de asistență online autoadministrate (Barak și colab., 2009, Dowling și Rickwood, 2013 cit in *idem*).

Printre diferitele forme de asistență prin Internet, **asistența online** se remarcă ca abordare de asistență la distanță care seamănă cel mai mult cu răspunsurile tradiționale de asistență, informații și / sau intervenție față în față.

Asistența online se referă la furnizarea de asistență și / sau informații pentru o victimă a infracțiunii în care (APAV, 2019):

- Comunicarea se realizează folosind internetul și TIC;
- Asistența și / sau informațiile sunt furnizate de la distanță (adică la distanță), acolo unde profesionistul și victima se află în spații fizice diferite;
- Comunicarea poate fi realizată în mod sincron (în timp real, cum este cazul serviciilor de chat și comunicării prin aplicații precum Skype® sau Whatsapp®) sau asincron (în cazul în care există un decalaj de timp între comunicarea de către victimă și răspunsul profesionistului, cum este cazul mesajelor e-mail sau al formularelor online).

În ciuda dovezilor puține despre eficiența internetului și a asistenței online, în special în intervențiile cu victimele infracțiunilor, au fost evidențiate mai multe avantaje și beneficii.

IMPORTANT | STATISTICI ÎN FOCUS

În cadrul Proiectului *T@LK* - sprijin online pentru victimele infracțiunilor, finanțat de Programul de justiție al Uniunii Europene, a fost realizat un sondaj cu privire la sprijinul la distanță și sprijinul online pentru victimele infracțiunilor cu 60 de organizații și servicii de sprijinire a victimelor din Europa. Printre alte subiecte, acest sondaj a explorat avantajele oferirii de asistență online victimelor infracțiunilor:

- 82% dintre organizațiile participante au menționat *accesibilitatea* la servicii de sprijin ca un avantaj.
- Aproximativ 80% din organizațiile participante cu sprijin online au indicat *comoditatea* și *flexibilitatea* în accesarea serviciilor de asistență drept avantaje, cu o proporție mai mică (58%) fără servicii de asistență online victimelor infracțiunilor, indicând comoditatea și flexibilitatea ca aspecte pozitive.
- *Accesul facilitat*, în special pentru victimele cu dificultăți în accesarea serviciilor de asistență convenționale, a fost indicat ca un avantaj de 60% din organizațiile participante cu servicii de asistență online pentru victimele infracțiunilor și de 74% din organizațiile participante fără servicii de asistență online.
- *Facilitarea primului contact al unei victime cu serviciile și organizațiile de sprijin* a fost indicată ca un avantaj de 71% dintre cei cu sprijin online, dar de doar 42% dintre cei fără servicii online pentru a sprijini victimele infracțiunilor.
- Un *număr mai mare de victime care pot accesa asistența* a fost indicat ca un avantaj de 79% dintre organizațiile participante fără servicii de asistență online, dar la o scară mai mică (57%) de organizațiile cu servicii de asistență online pentru victimele infracțiunilor.

Raportul complet cu informații detaliate despre acest rezultat și alte rezultate ale sondajului este disponibil la: https://www.apav.pt/publiproj/images/yootheme/PDF/TALK.pdf

IMPORTANT | PRACTICA ÎN FOCUS"

În cadrul aceluiași proiect, a fost dezvoltat Manualul T@LK - sprijin online pentru victimele infracțiunilor. Este un manual pentru organizațiile de sprijinire a victimelor, care le ajută să înțeleagă sprijinul prin intermediul internetului, precum și să creeze și / sau să pună în aplicare servicii de asistență online pentru victimele infracțiunilor.

Poate fi accesat la adresa https://www.apav.pt/publiproj/images/yootheme/PDF/Handbook_TALK.pdf

3.5. Sprijin din partea experților pentru victimele criminalității informatice

În urma intervenției, în special a unei intervenții de criză și ținând cont de informațiile furnizate de victima criminalității informatice și de nevoile de sprijin și protecție identificate, poate fi necesar să se trimită (intern sau extern) victima criminalității informatice la răspunsuri de sprijin specializate, în special la nivel legal , la nivel psihologic și social, pentru a minimiza consecințele criminalității informatice, pentru a reorganiza viața victimei și pentru a răspunde nevoilor acesteia.

3.5.1. Sprijin juridic: obiective și aspecte cheie

Sprijinul juridic pentru victimele infracțiunilor informatice ar trebui să fie oferit exclusiv de specialiștii în drept, dar este foarte util ca orice specialist în sprijin să fie conștient de cadrul juridic național și de alte instrumente juridice comunitare și internaționale privind regimul juridic aplicabil. În acest scop, se recomandă citirea și consultarea capitolului 2 din partea I a acestui manual, care acoperă cadrul legal al criminalității informatice.

De asemenea, este esențial ca specialistul de sprijin să fie conștient de diferitele etape ale procedurilor penale și de măsura în care acestea pot informa și sprijini victima în fiecare etapă și cu privire la drepturile lor de victimă a infracțiunilor.

Asistența juridică cuprinde informații și sarcini care permit specialistului să însoțească și să sprijine victima unei infracțiuni înainte, în timpul și după diferitele etape ale procesului penal.

Sprijinul juridic constă în:

- Informații despre tipurile de criminalitate informatică și cadrul legal al acestora;
- Informații și sfaturi cu privire la drepturile victimelor infracțiunilor;
- Sprijin în analiza sesizărilor instanței și în redactarea răspunsurilor;
- Sprijin pentru redactarea unei cereri de rambursare a cheltuielilor suportate ca urmare a participării la procedură;
- Susținerea redactării unei cereri pentru a explica absența acestora din acte judiciare;
- Sprijin pentru scrierea și depunerea unei plângeri / raport;
- Sprijin / însoțire de către specialistul de asistență atunci când prezintă o reclamație / raport;
- Sprijin în scrierea și depunerea unei cereri civile (atunci când victima o poate prezenta, mai degrabă decât un avocat);
- Susținerea în scrierea cererilor de aplicare a măsurilor de protecție.

3.5.1.1. Drepturile victimelor infracțiunilor

Un punct de plecare cheie în sprijinirea victimei unei infracțiuni este să se asigure că, în orice etapă a procesului penal, victima are **acces efectiv și își exercită drepturile în mod informat**.

Transpunerea în legislația națională a Directivei 2012/29/EU a Parlamentului European și a Consiliului din 25 octombrie 2012, care stabilește standarde minime privind drepturile, sprijinul și protecția victimelor infracțiunilor, urmărește să consolideze poziția victimelor și a nevoilor individuale de sprijin și protecție ale acestora în călătoria lor prin sistemul de justiție penală, subliniind datoria statelor de a proteja victimele infracțiunilor, rudele și prietenii lor de victimizarea secundară sau repetată, intimidare și / sau represalii. Această directivă întărește, de asemenea, rolul esențial al organizațiilor de sprijinire a victimelor, fie în rolul lor complementar, fie ca înlocuitor al statului, în asigurarea accesului la servicii de asistență calificate, gratuite și confidențiale sau ca un catalizator pentru exercitarea eficientă și informată a drepturilor de către victimele infracțiunilor.

Acest manual nu înlocuiește citirea directivei în întregime[81] și subliniază importanța cunoașterii complete a diferitelor drepturi acoperite de acest instrument.

Mai jos, prezentăm un rezumat al unora dintre aceste drepturi și subliniem, încă o dată, importanța citirii acestui instrument juridic, precum și consultarea informațiilor despre implementarea practică a acestor drepturi la http://www.infovictims.com/com/

Dreptul la informare
Dreptul la informare este fundamental deoarece permite victimei infracțiunii să participe în mod informat la procedurile penale și să își exercite drepturile. Victimele criminalității au dreptul de a primi informații cu privire la drepturile lor, în special atunci când intră pentru prima dată în contact cu forțele de securitate sau cu autoritățile judiciare:

- ce tip de sprijin pot primi și cine îl poate oferi;
- cum și unde să raporteze sau să se plângă de o infracțiune;
- cum și în ce circumstanțe pot solicita măsuri de protecție;
- cum pot obține consiliere juridică sau asistență juridică;
- cum și în ce circumstanțe pot solicita despăgubiri de la infractor;
- cum și în ce circumstanțe pot solicita despăgubiri de la stat;
- dacă victima nu vorbește limba utilizată în procesul penal sau are un handicap, cum poate primi servicii de interpretare și traducere;
- dacă nu locuiește în statul membru în care a avut loc infracțiunea, ce proceduri sunt în vigoare pentru ca aceasta să își exercite drepturile în țara respectivă;
- dacă autoritățile nu respectă drepturile victimei, unde poate merge victima pentru a depune o plângere;
- ce contacte ar trebui să utilizeze pentru a obține sau adăuga informații despre / la proces;
- ce servicii de mediere sunt disponibile;

[81] Documentul complet este disponibil la: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32012L0029.

- cum și în ce circumstanțe pot solicita rambursarea costurilor aferente participării lor la procedurile penale.

Dreptul de a primi dovada plângerii
O victimă care raportează o infracțiune sau depune o plângere la autoritatea competentă are dreptul să primească o dovadă a depunerii plângerii sau a reclamației.

Dreptul la traducere
Orice documente și acte care fac parte din procesul penal sunt, de regulă, în limba țării în care acesta are loc. Este un drept consacrat în directivă și, ulterior, al oricărei victime din orice stat membru că poate participa la procedurile penale oral și / sau în scris într-o limbă pe care o înțelege. Prin urmare, autoritatea responsabilă pentru un anumit proces penal trebuie să solicite asistența unui interpret sau traducător care înțelege atât limba procedurilor, cât și limba victimei. În funcție de rolul pe care îl are victima în procedură, adică o parte civilă sau asistent, ea are dreptul de a primi traduceri într-o limbă pe care o înțelege toate informațiile din procesul penal esențiale pentru exercitarea drepturilor sale. Atunci când victima are un handicap, are dreptul să primească interpretare într-o formă care să îi permită să participe eficient la proces, adică să solicite un interpret de limbaj al semnelor sau să solicite un răspuns scris la întrebări orale.

Dreptul de a accesa serviciile de sprijin pentru victime
Victima are dreptul de a accesa serviciile de asistență pentru victime, puse la dispoziție gratuit și confidențial, chiar dacă victima a ales să nu depună o plângere oficială sau să raporteze infracțiunea.

Dreptul de a fi auzit(ă)[82]
În timpul procesului penal, victima are dreptul de a fi audiată, de a pune la dispoziție informații importante pentru anchetă și de a furniza probe. Cu toate acestea, victima trebuie, în momentul raportării infracțiunii sau al depunerii unei plângeri, să pună la dispoziția autorității responsabile cât mai multe informații și probe relevante. Cu toate acestea, în timpul fazei de investigație, victima poate adăuga elemente suplimentare atunci când este chemată să facă declarații procurorului. Mai mult, dacă autorul infracțiunii este acuzat (inculpat) și cazul este trimis în judecată, victima poate adăuga informații suplimentare sau lipsă și poate răspunde la întrebările ridicate de diferitele părți implicate în caz.

De asemenea, este posibil ca victima, din cauza vulnerabilității sale particulare, să fie audiată în timpul fazei de anchetă, iar mărturia sa să fie înregistrată și utilizată în etapele ulterioare ale procesului penal, evitându-se astfel repetarea mărturiei victimei.

Drepturi dacă inculpatul nu este acuzat
Dacă, la sfârșitul fazei de anchetă, Parchetul constată că nu există probe suficiente pentru acuzarea și aducerea în judecată a acuzatului, dosarul penal este clasat. Dacă au fost comise mai multe infracțiuni, învinuitul poate fi pus sub acuzare doar pentru unele dintre infracțiuni, iar cazul va fi clasat pentru infracțiunile rămase.

În această situație și în cazul în care victima nu este de acord cu decizia, acesta are dreptul de a depune

[82] Acest drept, spre deosebire de precedentele, nu face parte din Directiva 2012/29/EU. Acesta este inclus în articolul 17 din Regulamentul general privind protecția datelor. Pentru informații suplimentare, consultați partea I, capitolul 2, secțiunea 2.2 din acest manual.

o cerere judecătorului de instrucție care solicită deschiderea unei anchete. Victima poate solicita, de asemenea, o reexaminare a probelor sau continuarea anchetei, la care poate prezenta noi dovezi.

Dreptul la servicii de mediere
În situații de gravitate mică și medie, cum ar fi amenințarea penală, leziuni minore, agresiuni sau altele, legea permite soluționarea cazului prin mediere între victimă și acuzat, dacă acesta din urmă a recunoscut săvârșirea infracțiunii.

Procesul de mediere ar trebui să fie gratuit, confidențial și voluntar, adică victima poate alege să participe sau nu în orice moment.

Scopul acestui proces este de a oferi un spațiu de comunicare, susținut și facilitat de un interlocutor imparțial, astfel încât victima să poată transmite impactul și / sau daunele cauzate de infracțiune și acuzatul să își asume responsabilitatea pentru faptă.

Mediatorul este un profesionist special instruit în domeniul medierii, iar atribuția lor este de a facilita comunicarea dintre participanți.

Dreptul la informare sau la protecția legală
Sistemul de acces la lege și la instanțe este conceput pentru a se asigura că nimeni nu are dificultăți sau este împiedicat, din cauza condiției lor culturale sau sociale, a mijloacelor sau cunoștințelor economice insuficiente, să își exercite și să-și apere drepturile.

Astfel, victima are dreptul la consiliere juridică cu privire la rolul său în procesul penal. Dacă victima este un asistent sau o parte civilă sau dacă victima dorește să fie însoțită de un avocat și nu are mijloacele financiare pentru a face acest lucru, are dreptul la asistență juridică, care poate consta în: renunțare totală sau parțială la plata taxei legale; numirea și plata onorariilor unui avocat; plata pe etape a onorariului legal sau a onorariilor avocatului.

Dreptul la despăgubire pentru participarea la procedură și rambursarea cheltuielilor
Orice victimă care participă la un dosar penal are dreptul la despăgubiri pentru timpul de participare, precum și la rambursarea cheltuielilor efectuate ca urmare a acestuia.

Dreptul la restituirea proprietății
În cazul în care obiectele sau alte bunuri deținute de victimă sunt reținute de autoritatea (autoritățile) competente ca probe și nu mai sunt necesare pentru procesul penal, acestea trebuie returnate fără întârziere. Această returnare ar trebui să aibă loc cât mai curând posibil, astfel încât victima să nu fie privată de bunurile sale mai mult decât este strict necesar în scopul procesului penal.

Dreptul la despăgubire
Oricine suferă daune ca urmare a unei infracțiuni are dreptul la despăgubiri.

Obligația de despăgubire revine infractorului sau, în circumstanțele în care infracțiunea lasă victima în dificultăți economice sau nu permite victimei să fie despăgubită la timp de către infractor, se poate face o cerere către stat pentru plata în avans a compensării.

Dreptul la protecție
Victimele și rudele acestora au dreptul la protecție împotriva actelor de represalii, intimidare sau activități infracționale continue împotriva lor. Acestea au dreptul să fie protejate de acte care le-ar putea pune în pericol viața, integritatea fizică, bunăstarea emoțională și psihologică și demnitatea atunci când depun mărturie.

În cazul în care autoritățile consideră că există o amenințare gravă de acte de răzbunare sau dovezi puternice că siguranța și viața privată a victimei pot fi perturbate grav și în mod intenționat, ar trebui să se asigure un nivel adecvat de protecție atât pentru victimă, cât și pentru familia lor sau alte persoane apropiate.

Protecția și securitatea victimelor pot fi protejate prin aplicarea uneia sau mai multor măsuri coercitive învinuitului ca restricții asupra libertății acuzatului, care pot fi aplicate în cursul procedurilor penale, dacă există pericolul de fugă, pericolul obținerii și păstrării dovezilor infracțiunii, un pericol pentru ordinea publică și / sau un pericol de continuare a activității infracționale.

În cazul în care viața victimei sau a altui martor, integritatea fizică sau mentală, libertatea sau bunurile de o valoare considerabilă sunt puse în pericol din cauza contribuției lor la ancheta și urmărirea penală a infracțiunii, pot solicita aplicarea unor măsuri de protecție.

Drepturile victimelor cu nevoi speciale de protecție
O victimă cu nevoi speciale de protecție este o persoană care, datorită caracteristicilor sale personale, tipului sau naturii infracțiunii suferite și / sau circumstanțelor în care a avut loc, este deosebit de vulnerabilă la victimizarea ulterioară, victimizarea secundară, intimidare sau represalii și, prin urmare, are nevoie de îngrijire, în special protecție.

Această vulnerabilitate ar trebui evaluată de la caz la caz, dar o atenție specială ar trebui acordată victimelor care au suferit un prejudiciu considerabil din cauza gravității și seriozității infracțiunii, victimelor infracțiunilor motivate de discriminare pe baza caracteristicilor personale și victimele a căror relație și dependență de infractor le fac deosebit de vulnerabile.

În consecință, victimele terorismului, criminalității organizate, traficului de persoane, violenței de gen, violenței în relații intime, violenței sexuale și infracțiunilor motivate de ură merită o atenție specială. Indiferent de tipul infracțiunii suferite, copiilor, persoanelor în vârstă și persoanelor bolnave sau cu dizabilități ar trebui să li se acorde o atenție deosebită la evaluarea vulnerabilității.

Dreptul de a fi uitat(ă)[82]
Acest drept oferă titularului său posibilitatea de a solicita, verbal sau în scris, operatorului de date să

îi șteargă datele personale. Acest drept poate fi exercitat ori de câte ori informațiile personale sunt considerate inadecvate, irelevante sau și-au pierdut relevanța.

3.5.1.2. Importanța conservării dovezilor digitale

„*Probele au funcția de a demonstra realitatea faptelor*" (articolul 341 din Codul civil portughez) și „obiectul probă se referă la *toate faptele relevante din punct de vedere juridic pentru existența sau inexistența infracțiunii, pedeapsibilitatea sau ne-pedepsibilitatea învinuitului și stabilirea pedepsei privative de libertate aplicabile sau a ordinului de detenție* "(articolul 124 (1) din Codul de procedură penală portughez). Dacă există o cerere civilă, faptele relevante pentru determinarea răspunderii civile (articolul 124 alineatele (1) și (2) din Codul de procedură penală portughez) *fac obiectul probelor*. În ceea ce privește principiul legalității probelor, în sistemul juridic portughez, articolul 125 din Codul de procedură penală prevede că „*dovezile care nu sunt interzise de lege vor fi admisibile*".

Deoarece acestea sunt infracțiuni care apar în lumea digitală, ancheta lor se confruntă cu mai multe obstacole (Martellozzo & Jane, 2017). Studiile și cercetătorii care se concentrează pe analiza **criminalității informatice** și a dificultăților în **raportarea / plângerea**[83] **și investigarea criminalității informatice** au indicat, printre altele, următoarele obstacole:

- „locul" unde a avut loc conduita criminală;
- identificarea făptuitorului (în special datorită anonimatului oferit de ecosistemul spațiului informatic și a impermanenței și volatilității dovezilor asupra comportamentelor lor, care pot fi ușor blocate, modificate, făcute inutile sau șterse);
- stabilirea cauzalității în cazurile care implică adesea autori și victime multiple și răspândite.

Cu alte cuvinte, aceste dificultăți în cadrul anchetei sunt arătate prin faptul că acest tip de infracțiune este transnațională, anonimă și variabilă (în continuă evoluție și cu noi forme de acțiune care apar în mod constant) (Santos, 2016; Holt & Bossler, 2015).

IMPORTANT | PRACTICA ÎN FOCUS:

Proiectul *SIRIUS*, condus de *Centrul European de Combatere a Terorismului și de Centrul European de Criminalitate Informatică* al Europol, în parteneriat cu *Eurojust și Rețeaua judiciară europeană*, își propune să ajute autoritățile să facă față complexității și volumului de informații într-un mediu online în schimbare rapidă.

Acest proiect vizează schimbul de cunoștințe prin evenimente și o platformă restricționată în care statele membre (și țările terțe cu un acord operațional cu EUROPOL) pot găsi informații actualizate și pot accesa dovezi digitale pentru investigații penale.

Informații suplimentare sunt disponibile la: www.europol.europa.eu/sirius

[83] În acest scop, consultați partea I, secțiunea 1.4 din acest manual, care tratează diferența dintre numărul de infracțiuni raportate și cele comise efectiv asociate cu criminalitatea informatică și motivele pentru care nu se raportează infracțiunile informatice.

În ceea ce privește dovezile, utilizarea TIC în activități criminale a popularizat dovezile digitale (Balkin și colab., 2007).

Într-adevăr, una dintre cele mai semnificative diferențe între criminalitatea informatică și criminalitatea tradițională se referă la natura probelor. Există diferențe în ceea ce privește forma, modul în care sunt stocate, locul în care sunt localizate și modul în care pot fi găsite. În plus, dovezile digitale sunt intangibile, în general volatile, iar cantitatea lor poate fi, de asemenea, masivă, ceea ce reprezintă provocări logistice substanțiale (Grabosky, 2007).

Deoarece dovezile digitale sunt temporare și extrem de volatile, există provocări suplimentare pentru a asigura validitatea acestora și pentru a proteja alte caracteristici relevante, adică este esențial să vă asigurați că dovezile sunt admisibile, autentice, exacte și complete (Marques, 2013). De exemplu, o simplă neconformitate în stocarea probelor și ruperea ulterioară a lanțului probelor o pot anula și o pot face inadmisibilă din punct de vedere legal (*idem*).

Dovezile digitale, la fel ca alte tipuri de dovezi, trebuie manipulate astfel încât să li se păstreze valoarea probatorie, care se referă nu numai la integritatea fizică, ci și la datele pe care le conțin. În funcție de tipul de dispozitiv, trebuie implementate măsuri speciale de colectare, ambalare, transport și depozitare (*idem*).

3.5.1.3. Rolul cooperării interinstituționale

Având în vedere natura intervenției cu victimele criminalității informatice și răspunsul la nevoile lor de sprijin identificate, care sunt adesea asociate cu procesul penal, este important să se ia în considerare **coordonarea interinstituțională între organizațiile și serviciile de sprijinire a victimelor și poliția și autoritățile judiciare**.

În mod ideal, aceste procese de colaborare interinstituțională ar putea fi realizate prin parteneriate formale via **protocoale și acorduri de cooperare**, care permit definirea în comun a procedurilor și a colaborării, pentru a eficientiza mecanismele de comunicare și schimbul de informații care contribuie la un mai bun sprijin, tratament și intervenție pentru victimele infracțiunilor în general și victimelor infracțiunilor informatice în special.

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

IMPORTANT | PRACTICA ÎN FOCUS:

Asociația Portugheză pentru Sprijinirea Victimelor (APAV) și Poliția Judiciară Portugheză, o autoritate care în Portugalia și-a rezervat competența în investigarea criminalității informatice, au semnat în 2019 un protocol de cooperare pentru colaborarea lor în cadrul Liniei de internet sigure (în portugheză: *Linha Internet Segura*).

Linia de Internet Sigur, operată de APAV în cadrul consorțiului Safe Internet Center, este un serviciu de asistență telefonică și online cu două componente: sfaturi și informații cu privire la problemele legate de utilizarea internetului și a TIC, precum și asistență și informații în situații de criminalitate informatică (Linie de asistență telefonică); raportarea de conținut ilegal pe Internet (Hotline).

Acest protocol de cooperare acoperă, de asemenea, stabilirea unui sistem de trimitere către APAV pentru victimele infracțiunilor informatice deservite de Poliția Judiciară și permite transmiterea eficientă a informațiilor legate de plângerile referitoare la infracțiuni informatice primite de Linia de internet securizată către Poliția Judiciară.

În general, și după cum confirmă exemplul de mai sus, aceste protocoale și acorduri promovează stabilirea și implementarea **mecanismelor de sesizare și referință a victimelor infracțiunilor**.

În acest sens, Directiva 2012/29/EU menționată anterior recomandă facilitarea sesizării victimelor infracțiunilor de către autoritățile competente către serviciile de sprijinire a victimelor pentru a asigura **dreptul victimei de a accesa serviciile de asistență înainte, în timpul și pe o perioadă adecvată după încheiere a procesului penal**.

În urma acestuia, vedem procesul **de referință ca un mecanism de colaborare interinstituțională** în care o organizație transmite informații despre apariția infracțiunilor și victimele acestora către o altă organizație, cu acordul victimei și pentru a le oferi sprijin. Referința diferă de recomandare, deoarece se bazează pe procese pro-active care fac parte integrantă din procedurile de sprijin pentru victimele infracțiunilor unui anumit serviciu sau organizație de sprijin. Referința implică întotdeauna respectul pentru voința și consimțământul victimei și promovează accesul victimei la un sprijin mai specializat sau specific, care va satisface cel mai bine nevoile identificate anterior.

IMPORTANT | INFORMAȚIE ÎN FOCUS:

Modul în care sunt colectate și transmise informațiile, care vizează referirea victimelor infracțiunilor, trebuie de asemenea stabilit și convenit între organizațiile implicate într-un anumit mecanism de referință.

Indiferent de metoda (metodele) de colectare și transmitere a informațiilor, este esențial ca informațiile transmise să permită identificarea victimei și înțelegerea situației de victimizare, minimizând riscul ca victima să fie nevoită să raporteze din nou episodul (episoadele) care a condus la contactul cu serviciul sau organizația de asistență.

Prin urmare, următoarele informații de bază ar trebui incluse în orice proces de referință:

- Numele victimei;
- Datele de contact ale victimei și timpul preferat pentru contact;
- Scurtă descriere a infracțiunii / situației de victimizare (tipul infracțiunii; relația cu infractorul, dacă este cazul; consecințele și impactul victimizării);
- Observații și sprijin furnizat de organizație (de exemplu, sprijin psihologic, informații juridice și alte observații relevante pentru organizația la care a fost trimisă victima).

3.5.2. uport psihologic: obiective și aspecte fundamentale

Sprijinul psihologic vizează furnizarea unei experiențe terapeutice victimei și / sau familiei și reducerea la minimum a efectelor negative ale expunerii la o experiență adversă și potențial traumatică. Astfel, răspunde nevoii victimei și / sau a familiei lor de a-și restabili funcționarea psihologică și emoțională și bunăstarea afectată de experiența victimizării (APAV, 2013b).

Sprijinul psihologic ar trebui oferit exclusiv de profesioniști cu diplomă în psihologie și ale căror calificări și experiență au fost recunoscute în mod corespunzător, după caz, de către entitatea de reglementare respectivă a țării, care reglementează accesul la profesie și activitatea profesională.

Există mai multe modele și școli utilizate în intervenția psihologică cu victimele infracțiunilor, inclusiv terapii psiho-dinamice, intervenții cognitiv-comportamentale și terapii narative și constructiviste. Indiferent de abordarea teoretică preferată a specialistului în asistență și a organizației sale, cunoștințele despre diferitele forme ale criminalității informatice și dinamica acesteia, precum și despre factorii de risc asociați cu criminalitatea informatică și impactul său asupra funcționării psihologice, emoționale și sociale a victimei sunt fundamentale[84].

Principalele obiective ale sprijinului psihologic sunt:

- Ameliorarea și îmbunătățirea simptomelor;
- Reducerea disconfortului și a comportamentului disfuncțional;

[84] Consultați, în acest scop, capitolele 1, 3 și 4 din partea I a acestui manual, în care tipologiile și diferitele tipuri de criminalitate informatică, factorii de risc socio-demografici și factorii de risc comportamental asociați cu experiența criminalității informatice și consecințele criminalității informatice sunt explorați.

- Consolidarea mecanismelor de apărare adaptive;
- Îmbunătățirea adaptării la mediu;
- Îmbunătățirea capacității de a judeca realitatea;
- Creșterea stimei de sine;
- Maximizarea autonomiei;
- Restabilirea echilibrului psihologic.

În secțiunile următoare, prezentăm orientări și câteva dintre aspectele cheie generice de luat în considerare atunci când oferim răspunsuri de asistență psihologică victimelor criminalității informatice. Conținutul acoperit nu reprezintă un program de intervenție referențială sau psihologică cu victimele criminalității informatice; mai degrabă, propune presupuneri și principii care ar trebui luate în considerare în orice proces de intervenție în acest domeniu, indiferent de abordarea teoretică utilizată și de organizația care oferă sprijin.

3.5.2.1. Cerințe și principii de operare ale sprijinului psihologic

Unele dintre **cerințele** care ar trebui luate în considerare pentru succesul intervenției psihologice cu victima sunt (APAV, 2013b; Alexy și colab., 2005):

- Specialistul ar trebui să stabilească o alianță terapeutică și o relație de susținere cu victima, fără stigmatizare și prejudecăți;
- Specialistul ar trebui să evalueze în mod adecvat impactul experienței de victimizare informatică, în special indicatorii de neadaptare psihologică, emoțională și comportamentală, inclusiv evitarea și retrăirea (simptome asociate cu stresul post- traumatic), funcționarea socială și comportamentul profesional și riscul de sinucidere;
- Specialistul ar trebui să evalueze, de asemenea, posibile comorbidități cu alte tulburări sau afecțiuni psihice, referind victima la alți profesioniști și / sau servicii mai specializate, dacă este necesar;
- Întrebările trebuie să fie la timp și sensibile, facilitând relatarea verbală a victimei;
- Specialistul ar trebui să valideze sentimentele, gândurile și istoricul victimizării victimei;
- Specialistul ar trebui să ajute victima să facă față emoțiilor și sentimentelor adverse asociate cu experiența de victimizare informatică, cum ar fi frica, furia, vinovăția și rușinea;
- Specialistul ar trebui să furnizeze informații despre posibilele reacții la experiența de victimizare informatică, fiind capabil să încadreze gândurile, sentimentele și comportamentele victimei ca reacții normale și consecințe la evenimente neașteptate de viață, promovând așteptări pozitive cu privire la procesul de recuperare;
- Specialistul ar trebui să ajute victima să găsească strategii de diminuare a evitării cognitive și comportamentale și să facă față în mod eficient posibilității de a retrăi evenimentul și apariția gândurilor intruzive, cum ar fi sentimentele de ineficiență, incompetență și lipsă de speranță, precum și furia, vinovăția. și rușine, promovând creșterea stimei de sine și stabilirea unor relații de încredere.

Următoarele **principii de funcționare** ar trebui, de asemenea, luate în considerare (APAV, 2011; APAV, 2013b):

Contract terapeutic
La începutul procesului de sprijin, un set de reguli și proceduri ar trebui să fie convenit cu victima - contractul terapeutic, care să definească timpul, frecvența și durata ședințelor, regulile de participare și punctualitate, precum și prezentarea obiectivelor și a planificării pentru intervenție. Acest contract are, de asemenea, scopul de a asigura angajarea și responsabilitatea victimei față de procesul de sprijin psihologic și succesele rezultate, contribuind la implicarea victimei și la respectarea obiectivelor intervenției.

Neutralitate și anonimat
Specialistul ar trebui să comunice și să interacționeze cu victima fără păreri personale, auto-revelații, manipulări și alte răspunsuri inadecvate de sprijin psihologic. Acestea ar trebui să promoveze exprimarea emoțională și afectivă liberă a victimei, fără jenă.

Neutralitatea nu înseamnă lipsă de empatie, iar această competență este foarte importantă pentru a construi o relație de încredere între victimă și profesionistul de sprijin, așa cum am menționat anterior[85].

Nedivulgarea și confidențialitate
Victima trebuie să fie asigurată că informațiile împărtășite în contextul sprijinului psihologic vor fi păstrate întotdeauna în sfera intervenției. Transmiterea informațiilor către terți (persoane sau organizații) despre asistența psihologică va avea loc numai după consimțământul prealabil al victimei prevăzut în acest scop specific.

3.5.2.2. Fazele procesului de sprijin psihologic

faza inițială | relația terapeutică și colectarea informațiilor

faza de dezvoltare | implementarea planului de intervenție psihologică

faza de terminare | verificarea dacă obiectivele intenționate și modificările au fost atinse

Faza inițială a procesului de sprijin psihologic

Această fază vizează stabilirea unei relații de încredere între victimă și specialistul de sprijin responsabil cu intervenția psihologică. Aptitudinile personale și tehnice ale specialistului, precum și competențele sale empatice de comunicare (consultați secțiunile 2.1 și 2.2 din capitolul 2 din partea I a acestui manual) sunt fundamentale aici. În acest moment al procesului de sprijin se stabilește contractul terapeutic.

[85] Pentru informații suplimentare despre comunicare și empatie în contactele cu victimele infracțiunilor și criminalității informatice, vă rugăm să consultați capitolul 2 din această parte a manualului.

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

În faza inițială a acestui proces de intervenție, colectarea și analiza informațiilor ar trebui să aibă loc și să informeze un plan și strategii de intervenție psihologică.

În acest sens, **colectarea de informații** de la victima infracțiunii informatice de către (posibil) alți profesioniști de sprijin, în contactele anterioare cu organizația, poate fi utilă, deoarece oferă o înțelegere globală a istoriei vieții victimei, a resurselor interne și externe, precum și experiența criminalității informatice și impactul acesteia.

În plus, profesionistul poate utiliza **scripturi și interviuri pentru a colecta informații și instrumente de evaluare psihologică** pentru a înregistra și sistematiza informațiile relevante pentru stabilirea intervenției (în special pentru a răspunde solicitărilor victimei și a nevoilor lor emoționale și psihologice) și pentru a analiza domenii specifice de (dis)funcționalitate psihologică și emoțională. Colectarea informațiilor de la victime ar trebui completată prin observarea comportamentului și a **comunicării sale non-verbale și a limbajului** său, care sunt indicatori importanți asupra stării emoționale a victimei și a bunăstării și funcționării acestora.

Colectarea informațiilor pentru definirea intervenției psihologice poate fi, în sine, un proces terapeutic - în timp ce permite cartografierea resurselor (interne și externe) afectate de experiența de victimizare informatică, contribuie și la exprimarea emoțională liberă a victimei și la dezvoltarea o narațiune în jurul experienței de victimizare informatică.

Faza de dezvoltare a procesului de sprijin psihologic

Această fază este marcată de **implementarea planului de intervenție psihologică și a strategiilor** definite anterior și poate avea loc în mai multe ocazii sau sesiuni. De asemenea, continuă colectarea și analiza informațiilor, văzute ca un proces de intervenție circular și transversal.

Indiferent de strategiile de intervenție și de orientarea teoretică / paradigmatică utilizate, atunci când implementează planul de intervenție psihologică, specialistul de sprijin ar trebui să caute:

- **să faciliteze exprimarea emoțională și comunicarea**: specialistul ar trebui să motiveze victima să-și împărtășească sentimentele, emoțiile și gândurile, asigurându-le și arătând că acest lucru se poate face fără ca acestea să fie judecate;
- **să promoveze înțelegerea victimei cu privire la problemele și răspunsurile sale**: specialistul ar trebui să explice victimei tipul de infracțiune la care a fost supusă și să prezinte situații similare de victimizare informatică, facilitând victimei identificarea acestora cu istoricul victimizării și, ulterior, , cu nevoile și problemele asociate și soluțiile posibile;
- **să arate interes și empatie**: despre acest subiect, consultați partea II, capitolul 2, secțiunile 2.1 și 2.2 din acest manual;
- **să consolideze stimei de sine**: întărirea stimei de sine a victimei contribuie la promovarea schimbărilor de comportament dorite;
- **să faciliteze rezolvarea problemelor**: specialistul ar trebui să ajute victima să facă față dificultăților, să ia decizii și să rezolve problemele ghidând-o spre soluții.

Faza de terminare a procesului de sprijin psihologic

Deoarece este dificil să se determine momentul potrivit pentru a încheia procesul de sprijin psihologic, specialistul ar trebui să revizuiască împreună cu victima obiectivele planului de intervenție dezvoltate la început pentru:

- a afla ce semnificație atribuie victima experienței sale de victimizare informatică și în ce măsură consideră că obiectivele au fost îndeplinite în totalitate sau parțial;
- a anticipa strategiile de prevenire și protecție;
- a confirma ce abilități a dobândit victima pentru a menține îmbunătățirile și schimbările realizate prin procesul de intervenție.

După încheierea procesului, este important ca specialistul să asigure o urmărire a cazului pentru a colecta informații cu privire la faptul dacă rezultatele obținute după încheierea sprijinului psihologic sunt încă menținute.

Indiferent de momentul sau faza procesului de suport psihologic, tabelul următor prezintă câteva tehnici de comunicare care pot ajuta la realizarea obiectivelor intervențiilor (APAV, 2013b).

Tabel 7: Tehnici și strategii de comunicare utile pentru procesul de sprijin psihologic

Catharsis - facilitarea exprimării sentimentelor și emoțiilor
Întrebări - adresarea de întrebări închise (de ex. „Care este numele tău?") sau întrebări deschise (de ex. „Ce crezi despre asta?") pentru a obține informații
Restructurarea - reorganizarea informațiilor împărtășite de victimă într-un mod diferit, permițând o schimbare de perspectivă asupra subiectului
Focus - selectați, din informațiile împărtășite de victimă, cele mai relevante pentru un anumit obiectiv de intervenție
Interpretare - adăugarea de semnificație la ceva care a fost exprimat de victimă
Clarificare - a clarifica ceea ce a spus victima, pentru o mai bună înțelegere a simptomelor, sentimentelor și comportamentelor acestora
Confruntare - compararea conținutului discrepant pe același subiect pentru a clarifica îndoielile, incongruențele și / sau a contesta verbalizările sau comportamentele victimei
Sugestie - Inducerea unei idei sau a unui sentiment pentru a sugera scenarii alternative
Ecou - repetarea unui cuvânt sau întrebare despre unele informații împărtășite de victimă, ca o modalitate de a păstra atenția victimei asupra procesului de intervenție și de a consolida comunicarea empatică și relația dintre specialist și victimă
Tăcerea - servește în principal pentru a asigura timp pentru reflecție
Asigurarea stimei de sine - liniștirea și întărirea stimei de sine a victimei prin exprimarea acordului cu o idee, gând, atitudine sau decizie
Consiliere - prezentarea de atitudini sau decizii pentru a consolida aspecte sănătoase ale comportamentului victimei, a reduce simptomele sau a evita crizele
Educație - Clarificarea problemelor sau situațiilor relevante

3.5.3. Sprijin social: obiective și aspecte fundamentale

Conform Federației Internaționale a Asistenților Sociali (2005 cit. în APAV, 2013b), asistența socială include promovarea schimbărilor sociale, rezolvarea problemelor în contextul relațiilor interpersonale și a capacității oamenilor de a-și îmbunătăți bunăstarea. Asistența socială urmărește astfel să aducă **schimbări pozitive în funcționarea psihologică și socială a oamenilor, grupurilor și comunităților**, reducând vulnerabilitățile și oferind oportunități pentru o viață socială mai satisfăcătoare.

Scopurile de asistență socială sunt:

- Promovarea incluziunii grupurilor sociale vulnerabile sau cu risc;
- Promovarea bunăstării și rezolvarea problemelor prin intervenția cu oamenii, grupurile și comunitățile;
- Inițierea procedurilor de protecție pentru persoanele care, din cauza stării sau situației lor, nu sunt capabile să facă acest lucru în mod autonom.

Asistența socială se extinde, prin urmare, la domenii foarte diverse, cum ar fi educația, informarea și îndrumarea, sprijinul psihosocial și gestionarea serviciilor sau echipamentelor (APAV, 2013b).

Asistența socială este în responsabilitatea lucrătorilor sociali, dar și a specialiștilor în politici sociale și a altor specialiști calificați corespunzător în zona de asistență socială (*idem*).

Ca și în cazul altor forme specializate de sprijin, sprijinul social pentru victimele criminalității informatice necesită ca specialiștii, pe lângă pregătirea lor academică, să cunoască și să stăpânească cadrul teoretic și conceptual al nevoilor victimelor criminalității informatice. Mai mult, ei ar trebui să aibă cunoștințe adecvate și stăpânire a caracteristicilor și dinamicii asociate diferitelor tipuri de criminalitate informatică și impactul acestora asupra victimelor[86].

3.5.3.1. De la diagnosticul social la intervenția individualizată

Diagnosticul social este un proces de elaborare / sistematizare a informațiilor despre un context, înțelegând problemele și nevoile acestuia, precum și cauzele și evoluția acestora. Prin diagnostic social, este posibil să se stabilească priorități și strategii de intervenție, **implicând resursele disponibile și actorii sociali** (Ander-Egg & Idánez, 1999 cit în APAV, 2018).

Diagnosticul social ar trebui să fie una dintre primele faze ale sprijinului social. Reprezintă un proces continuu, care vizează cunoașterea realității trăite de o anumită persoană, grup sau comunitate, precum și evoluțiile / modificările sale constante, necesitând astfel o colectare și o analiză constantă a informațiilor.

Diagnosticul social este un pas de bază pentru o intervenție individualizată cu victima criminalității și a criminalității informatice. Doar după diagnosticarea situației relaționale, sociale și instituționale a

[86] Consultați capitolele 1, 3 și 4 din partea I a acestui manual, care explorează, pe rând, tipologiile și diferitele tipuri de criminalitate informatică, factorii de risc asociați cu experiența criminalității informatice, consecințele criminalității informatice și nevoile victimelor criminalității informatice.

victimei, profesionistul ar trebui să proiecteze intervenția, implicând victima și rețeaua sa principală de sprijin, precum și structurile formale de sprijin (García & Romero, 2012 cit în APAV, 2018). Această abordare a intervenției individualizate se numește Metodă de caz.

Metoda cazului poate fi rezumată în patru pași de bază (*idem*):

- Studiul și diagnosticarea problemei;
- Proiectarea programului / intervenției;
- Livrarea / implementarea intervenției;
- Evaluarea.

Pentru a realiza aceste patru etape, care vor produce o intervenție individualizată axată pe nevoile relaționale, sociale și instituționale ale victimei, specialistul ar trebui:

3. OFERIREA DE SPRIJIN VICTIMELOR INFRACȚIUNILOR INFORMATICE

Să identifice infracțiunea

Identificarea victimei și a infracțiunii se poate baza pe informațiile colectate din alte contacte dintre victimă și organizație și include experiența / istoricul victimizării informatice, informații despre victimă, caracterizarea acestora și istoricul pre-victimizării.

Să evalueze nevoile victimei

Evaluarea nevoilor individuale și sociale ale victimei ar trebui să se concentreze asupra intereselor acestora, în funcție de contextul său de viață și luând în considerare problemele specifice ale cazului său.

Specialistul trebuie să:

- Permită victimei să exprime ceea ce își dorește și de ce are nevoie;
- Clarifice și reformuleze nevoilor exprimate pentru a asigura o înțelegere corectă;
- Furnizeze în continuu informații cu privire la drepturile, resursele și serviciile de sprijin existente care permit victimelor să își identifice propriile nevoi;
- Evalueze continuu diferitele nevoi și nivelurile lor de urgență pentru a răspunde celor mai presante.

Nevoile urgente includ: siguranță, nevoi de bază, îngrijire medicală și / sau psihologică, adăpost și asistență juridică.

Nevoile pe termen mediu și / sau lung pot include: sprijin financiar, susținerea educației acestora, sprijin (re) integrării, formarea competențelor și integrarea profesională.

De regulă, nevoile de asistență socială pot fi grupate în următoarele dimensiuni:

ADAPOST	Situațiile de criminalitate informatică motivate de relații, permise prin Internet și TIC, cum ar fi urmărirea online și difuzarea non-consensuală a imaginilor și videoclipurilor în situații de violență în relațiile intime, pot necesita adăpost, fie urgent / de urgență, fie sprijin planificat. Specialistul ar trebui să pregătească un diagnostic de situație (să identifice rețeaua principală de asistență - prieteni, rude și alte persoane de încredere - sau necesitatea activării rețelelor secundare de asistență) și să evalueze gradul de risc al situației. Asistența poate avea loc în rețeaua principală de asistență, dacă îndeplinește condițiile de siguranță necesare. Poate fi, de asemenea, instituțional, ceea ce necesită conștientizarea adăpostului disponibil la nivel local / regional / național și trimiterea către liniile de urgență socială, structurile / răspunsurile adăposturilor, organizațiile neguvernamentale, serviciile de securitate socială, printre alte răspunsuri / resurse disponibile.
MANCARE	Victima criminalității informatice, de exemplu, în escrocheriile online, se poate afla în situații de insuficiență economică și incapabil(ă) să își satisfacă nevoile de bază, cum ar fi hrana sau medicamentele pentru probleme de sănătate preexistente. Specialistul ar trebui să cartografieze diferitele instituții din acea zonă de intervenție, obiectivele, procedurile și regulile de funcționare ale acestora, pentru a îndruma victima în mod adecvat, însoțindu-le atunci când contactează aceste alte organizații. În acest scop, specialistul ar trebui să cunoască organizațiile din propria țară care pot fi contactate pentru a răspunde acestor nevoi și, în cele din urmă, să facă trimiteri către organizații neguvernamentale, servicii de securitate socială, instituții religioase, printre alte răspunsuri / resurse disponibile.

SANATATE	Experiența victimizării informatice poate duce la nevoi de sănătate fizică sau mentală. Specialistul ar trebui să poată identifica cele mai adecvate organizații și răspunsuri din propria țară și, eventual, să facă trimiteri către liniile de sănătate / urgență, serviciile de sănătate finanțate de stat, organizațiile neguvernamentale, organismele religioase sau alte răspunsuri din domeniul sănătății (inclusiv furnizori privați de servicii de sănătate).
SITUATIA OCUPATIONALA	Având în vedere efectele potențiale ale criminalității informatice asupra situației profesionale a victimei, poate fi necesar să se găsească o nouă modalitate de asigurare a mijloacelor de trai ale acesteia. (Re-)Integrarea profesională devine esențială pentru a permite un nivel mai înalt de autonomie. Specialistul ar trebui să evalueze calificările academice ale victimei, experiența sa profesională, preferințele sale cu privire la sectoarele pieței muncii și posibilele nevoi de formare. Specialistul ar trebui să trimită victima către organisme competente, cum ar fi centrele de angajare și formare profesională, care pot ajuta și promova reintegrarea profesională. De asemenea, acestea ar trebui să faciliteze victima să contacteze departamentele de resurse umane în zonele de lucru care se potrivesc profilului, abilităților și intereselor de muncă ale victimei.
SITUATIA EDUCATIONALA / DE FORMARE	Criminalitatea informatică poate afecta situația educațională a copilului sau tânărului victimă în situații precum agresiunea informatică, abuzul și exploatarea sexuală a copiilor online sau copiii și tinerii aflați în grija victimei directe a criminalității informatice (dacă acest lucru se aplică cazului specific). Este important ca specialistul să aibă legături cu instituțiile actuale de formare sau educație pentru a implementa acțiuni care să răspundă nevoilor de formare directă și indirectă ale victimelor, cum ar fi transferul la o altă școală sau un program de formare, care ar trebui făcut discret pentru a garanta siguranța victime directe și indirecte.

Să trimită mai departe și să lucreze în mod colaborativ

Aceste nevoi de bază (și răspunsurile la acestea) sunt domenii importante de intervenție în ceea ce privește sprijinul social.

Având în vedere nevoile identificate și sfera de acțiune a organizației specialistului, poate fi necesar, așa cum s-a menționat mai sus, să trimită victima și să colaboreze cu alte organizații / servicii din comunitate. Specialiștii (și organizația lor) ar trebui să aibă, pentru fiecare domeniu de intervenție, contacte ale rețelelor secundare de sprijin existente la nivel regional și național, care pot fi activate pentru a sprijini nevoile victimelor infracțiunilor.

Pentru a răspunde nevoilor victimei și pentru a maximiza calitatea asistenței oferite, ar putea fi necesară legătura cu alte sectoare / domenii, în special:

- Securitatea socială și protecția socială (cum ar fi serviciile de securitate socială și organizațiile de caritate private / organizațiile neguvernamentale);
- Muncă și șomaj (inclusiv locuri de muncă și centre de formare profesională);
- Departamentele de resurse umane ale companiilor și ale altor organizații sau comitete locale;
- Sănătate (cum ar fi spitale, centre / unități de sănătate și instituții de sănătate mintală);
- Instituții de educație și / sau instruire;
- Autoritățile locale (de exemplu, consiliile municipale și consiliile parohiale);
- Justiție (cum ar fi forțele de poliție, instanțele judecătorești și oficiile criminalistice);
- Comunicații și TIC (inclusiv operatorii de telecomunicații, furnizorii de servicii Internet, furnizorii de platforme de rețele sociale și alte platforme de partajare a informațiilor);
- Economia și finanțele (cum ar fi băncile, instituțiile de credit și companiile sau platformele de plăți și transferuri electronice).

Legătura cu aceste servicii poate avea loc ca referire sau referință[87].

[87] Pentru mai multe informații despre referință și trimitere, vă rugăm să consultați partea II, capitolul 3, punctul 3.5.1.3 din acest manual, unde este abordată importanța colaborării interinstituționale.

3.5.3.2. Aspecte cheie pentru succesul muncii colaborative

Cooperarea interinstituțională este importantă în sprijinirea victimelor criminalității informatice, indiferent de sprijinul luat în considerare și este deosebit de relevantă în abordarea nevoilor sociale și instituționale identificate în urma unei experiențe de victimizare (sau a victimizării informatice, în acest caz).

Lucrul în colaborare cu specialiști din alte instituții și servicii este fundamental pentru calitatea tratamentului acordat oricărei victime a infracțiunilor.

Specialistul ar trebui să lucreze în colaborare constantă cu specialiști din alte instituții și servicii pentru a asigura un sprijin corect și un răspuns adecvat la interesele și nevoile victimei. Specialiștii ar trebui:

- **Să faciliteze**, prin promovarea unei comunicări eficiente și a unei relații satisfăcătoare între profesioniștii din diferite servicii și instituții;

- **Să stimuleze**, implicând acei specialiști în soluționarea / minimizarea consecințelor infracțiunilor sau a criminalității informatice și pentru a răspunde în mod adecvat la nevoile victimei.

Acțiunea integrată poate preveni unele dintre constrângerile care afectează colaborarea interinstituțională:

Formalismul. Efectele negative ale unui formalism excesiv asupra contactului zilnic dintre instituții (de exemplu, proceduri birocratice excesive) ar trebui reduse, deoarece acest lucru poate fi în detrimentul procesului de sprijin, în special rapiditatea și eficiența în soluționarea problemei.

Timpul. Timpul disponibil pentru îndeplinirea unei anumite cerințe a procesului (de exemplu, trimiterea rapidă a unui raport de trimitere) ar trebui gestionat eficient, fără a întârzia sau a submina activitatea altor servicii și instituții.

Lipsa simțului practic. O viziune practică a cerințelor procesului de sprijin ar trebui promovată atunci când contactați alte instituții.

Lipsa de cordialitate. Specialistul ar trebui să fie politicos cu toți profesioniștii în procesul de asistență cu care este în contact (de exemplu, la telefon, în persoană, prin e-mail etc.).

Erori de comunicare. Comunicările ambigue care conduc la o neînțelegere a mesajelor sau cererilor ar trebui evitate, deoarece acestea pot afecta relația și pot provoca daune considerabile, influențând calitatea sprijinului acordat victimei.

Partajarea insuficientă a informațiilor. Informațiile insuficiente împărtășite cu specialiștii din alte instituții sau servicii ar trebui evitate, deoarece acest lucru le poate limita sau întârzia munca în procesul de susținere (de exemplu, trimiterea unui raport neglijent, omisiv sau neclar care nu are

informațiile necesare pentru a progresa cu procesul).

Intervenție reductivă și izolată. Ar trebui adoptată o viziune globală în sprijinirea și sesizarea victimelor, promovând crearea de rețele prin participarea activă a altor profesioniști din afara serviciului sau instituției, optimizând resursele disponibile.

Concurență negativă. Nu ar trebui promovată o cultură a concurenței cu alte servicii și instituții; mai degrabă ar trebui să promovăm o cultură axată pe maximizarea resurselor și abilităților altor servicii și instituții pentru a promova o intervenție adecvată și de calitate.

Lipsa contactului personal. În cele din urmă, ar trebui să contactați personal specialiști din alte instituții și servicii, promovând relații de lucru strânse între toți, pentru a asigura mai ușor pașii necesari în intervenția ce privește victimele.

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

În general, **prevenirea criminalității** este definită ca toate inițiativele și eforturile private și / sau publice care vizează prevenirea criminalității prin reducerea riscului de apariție prin schimbarea factorilor de risc și / sau, atunci când acest lucru nu este posibil, prin atenuarea efectelor sale asupra oamenilor și societății (Copibianco, 2010, Welsh & Farrington, 2012 cit în Maia și colab., 2016).

Primele încercări de prevenire a criminalității provin din abordări de sănătate publică, iar conceptul de *prevenire* (de boală sau vătămare) a fost ulterior însușit de alte domenii ale vieții sociale și comunitare (Bloom, 1996, Doll, Saul și Elder, 2007 cit în Saavedra & Machado, 2010) și chiar transpuse la probleme legate de securitate, violență și criminalitate.

4.1. Abordări pentru prevenirea criminalității informatice: aspecte cheie

Urmând conceptul de prevenire menționat mai sus și o abordare a sănătății publice (APAV, 2011), prevenirea poate fi clasificată în funcție de ***momentul său*** (sau de evoluția afecțiunii) în următoarele dimensiuni:

- **Prevenire primară**: intervenție înainte de problemă, pentru a preveni apariția bolii sau a rănirii.
- **Prevenirea secundară**: intervenție menită să trateze problema, care a început, în cel mai devreme stadiu posibil.

  Transpunând-o la probleme de violență și criminalitate, prevenirea secundară se referă la abordări care se concentrează asupra reacțiilor imediate la criminalitate și violență (de exemplu, îngrijire medicală; servicii de urgență).
- **Prevenirea terțiară**: intervenție axată pe prevenirea recidivelor, prevenirea frecvenței și severității daunelor.

  Prevenirea terțiară, atunci când se aplică problemelor de violență și criminalitate, include abordări axate pe îngrijirea pe termen lung după violență sau criminalitate, cum ar fi reabilitarea, reintegrarea și reducerea traumei / consecințelor asociate cu infracțiunile / violența.

Deși în mod tradițional abordările de prevenire a criminalității și violenței secundare și terțiare sunt utilizate în intervenția cu victimele, acestea sunt considerate relevante și pentru intervenția cu autorii infracțiunilor sau violenței, în special în contextul răspunsurilor din sectorul judiciar.

Prevenirea poate fi, de asemenea, definită în funcție de grupul țintă de interes sau populație pentru care este destinată (APAV, 2011) și clasificată ca:

- **Prevenire universală**: abordări care vizează grupurile sau populația generală, indiferent de nivelul de risc.

  Exemple de abordări universale de prevenire includ programe de prevenire a violenței pentru copii și tineri la un anumit nivel școlar, precum și campanii de sensibilizare a populației.

- **Prevenirea selectivă**: abordări adresate grupurilor / persoanelor considerate a fi expuse unui risc mai mare de implicare în violență sau infracțiuni comparativ cu populația generală.

  Exemple ale acestei abordări de intervenție includ programe de promovare a abilităților parentale pentru părinții singuri.

- **Prevenire indicată**: abordări de intervenție pentru persoanele / grupurile cu risc crescut care au demonstrat deja o anumită implicare în situații de violență sau infracțiuni, fie ca victime și / sau făptași.

  De exemplu, abordările de prevenire indicate pot include programe de intervenție pentru persoanele acuzate de violență domestică și răspunsurile de sprijin pentru victimele infracțiunilor și violenței furnizate de organizațiile de sprijinire a victimelor.

Există, de asemenea, alte tipuri de clasificare a strategiilor de prevenire, și anume în funcție de ***focusul prevenirii*** (de exemplu, ONU, 2011 cit în Maia și colab., 2016; Tonry & Farrington, 1995 cit în Maia și colab., 2016):

- **Prevenirea criminalității prin dezvoltarea socială**, concentrându-se pe creșterea factorilor de protecție și reducerea factorilor de risc al criminalității, care pot include, de exemplu, programe de dezvoltare a abilităților sociale pentru copiii aflați în situații de risc.

- **Prevenirea criminalității comunitare sau locale**, concentrându-se pe intervenția în zone geografice cu un risc mai mare de criminalitate și promovând un sentiment de securitate.

- **Prevenirea situațională a criminalității**, care se referă la reducerea oportunităților de a comite infracțiuni, la creșterea riscurilor / costurilor asociate comiterii acesteia și la reducerea beneficiilor.

- **Prevenirea penală prin justiție penală**, care ar putea include reintegrarea și programe de prevenire a infractorilor recidiviști.

În afară de strategiile comunitare sau locale de prevenire a criminalității, celelalte abordări de prevenire a criminalității menționate mai sus pot fi traduse în prevenirea **criminalității informatice**. Este important de reținut că eforturile de prevenire a criminalității informatice se concentrează adesea pe tehnologie și protecția computerelor și dispozitivelor, în timp ce modelele de prevenire a criminalității se concentrează în primul rând pe factorul uman.

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

Indiferent de abordările de prevenire și de tipologiile rezumate mai sus, abordarea de sănătate publică[88] este utilă pentru a ajuta organizațiile să înțeleagă și să implementeze strategii de prevenire a criminalității și violenței. În ciuda complexității prevenirii, putem organiza planificarea, pregătirea și implementarea strategiilor de prevenire în patru macro-etape:

1 definirea problemei	• necesită înțelegerea fenomenului și dinamica acestuia și identificarea amplorii și expresiei acestuia (de exemplu, statistici privind numărul de rapoarte / plângeri privind o anumită infracțiune) într-un anumit grup, comunitate, regiune sau țară
2 identificarea factorilor de risc și a factorilor de protecție	• factori de risc: caracteristici sau condiții care pot crește probabilitatea unei anumite probleme • factori de protecție: caracteristici sau condiții care pot reduce probabilitatea unei anumite probleme • strategiile de prevenire ar trebui să reducă factorii de risc și să sporească factorii de protecție
3 elaborerea, testarea și evaluarea de strategii de prevenire	• strategiile de prevenire ar trebui să fie bazate pe dovezi, să ia în considerare diagnosticele care au fost efectuate, precum și problema care trebuie abordată și factorii de risc și de protecție asociați • monitorizarea strategiilor de prevenire și evaluarea eficienței acestora sunt pași cheie
4 mediatizare și generalizare	• după analiza rezultatelor strategiilor de prevenire implementate, este fundamental să le mediatizati pentru a permite utilizarea lor de către alte organizații

În plus, și în ceea ce privește prevenirea criminalității informatice, modelul propus de Askerniya (2012) pentru **organizarea strategiilor de prevenire** a criminalității informatice are patru dimensiuni cheie, toate incluzând conștientizarea și educația ca elemente critice în reducerea criminalității informatice (Jahankhani, 2013 cit în Al-Ali și colab., 2018):

1. **Nivelul de cunoștințe tehnice al utilizatorilor individuali** este prima dimensiune a intervențiilor de prevenire a criminalității informatice. Pentru a reduce riscul individual și a îmbunătăți protecția personală, intervențiile ar trebui să se concentreze pe educarea, sensibilizarea și instruirea utilizatorilor cu privire la abilitățile specifice necesare unei participări sigure la diferite activități online (cum ar fi descărcarea de muzică, jocuri și filme, cumpărături online și / sau folosind rețelele sociale).

2. A doua dimensiune se referă la reducerea expunerii la riscul de criminalitate informatică prin **strategii de prevenire adaptate diferitelor etape individuale de dezvoltare ale utilizatorului**. Această dimensiune presupune că riscul de criminalitate informatică este afectat de factorii de risc și de protecție asociați cu dezvoltarea individuală, astfel încât vârsta / grupa de vârstă a utilizatorului este esențială pentru a defini și a decide ce strategii de intervenție preventivă împotriva criminalității informatice ar trebui să fie livrate.

3. A treia dimensiune se referă la **nivelurile de risc ale utilizatorilor în ceea ce privește**

[88] Informații detaliate cu privire la abordarea de sănătate publică a prevenirii criminalității și violenței, precum și resurse pentru a sprijini planificarea, implementarea și evaluarea măsurilor de prevenire sunt disponibile la https://vetoviolence.cdc.gov/apps/main/home

expunerea lor la criminalitatea informatică și la necesitatea intervențiilor preventive în funcție de cunoștințele, instruirea și conștientizarea utilizatorilor. Prin urmare:

- **Riscul redus de expunere la criminalitatea informatică** este asociat cu utilizatorii care au cunoștințe considerabile despre TIC și Internet, precum și niveluri ajustate de conștientizare cu privire la riscurile expunerii online.

- **Riscul mediu de expunere la criminalitatea informatică** este asociat cu utilizatorii cu cunoștințe insuficiente și conștientizare a riscurilor de expunere online și cu un risc mai mare de victimizare informatică (comparativ cu categoria anterioară). Această dimensiune include persoanele care, în ciuda cunoștințelor lor despre securitatea computerelor și dispozitivelor, nu sunt suficient de conștiente pentru a-și schimba comportamentul online și / sau obiceiurile de utilizare a internetului și TIC.

- **Riscul ridicat de expunere la criminalitatea informatică** este asociat cu utilizatorii cu rate ridicate de utilizare intensivă a internetului și a TIC, dar conștientizarea scăzută a expunerii la risc.

4. Cea de-a patra și cea din urmă dimensiune a acestui model se referă la **promovarea abilităților și comportamentelor individuale și dezvoltarea intervențiilor** bazate pe instruire, educație și conștientizarea riscurilor în ceea ce privește riscurile de expunere online și comportamente specifice[89].

În secțiunea următoare vă prezentăm câteva practici de prevenire a criminalității informatice.

4.2. Informarea, conștientizarea și educația ca strategii de prevenire

Urmând dimensiunile cheie ale strategiilor de prevenire a criminalității informatice prezentate mai sus, devine clar cât de mare impact au informațiile, conștientizarea și educația utilizatorilor de Internet și TIC asupra comportamentului și abilităților lor și, în consecință, asupra creșterii / reducerii riscului de expunere la criminalitatea informatică.

Percepțiile utilizatorilor de internet și TIC despre propriile **abilități și cunoștințe** pentru a se proteja de victimizarea informatică le afectează comportamentul și activitățile online. Același lucru se aplică responsabilității pentru securitatea online personală (Boehmer și colab., 2015; LaRose și Rifon, 2007). Adică, persoanele care consideră că securitatea informatică este o responsabilitate personală și / sau care înțeleg că au cunoștințele și abilitățile necesare pentru a se proteja împotriva victimizării informatice adoptă (probabil) mai multe măsuri de securitate informatică și mai multe comportamente de protecție personală atunci când utilizează internetul și TIC.

[89] Pentru informații suplimentare referitoare la vulnerabilitate ca factor de risc pentru victimizarea informatică, vă rugăm să consultați partea I, capitolul 3, secțiunea 3.2 din acest manual.

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

Această interpretare evidențiază nevoia de **campanii de informare și conștientizare și programe educaționale** (Martin & Rice, 2011; Burns & Roberts, 2013):

- Campaniile de informare și conștientizare ar trebui să promoveze utilizarea sigură și competentă a internetului și a TIC;
- Programele educaționale ar trebui să ofere cunoștințe și oportunități pentru formarea și dobândirea abilităților necesare adoptării comportamentelor de siguranță online.

În orice caz, aceste strategii de informare, conștientizare și educație ar trebui (Bandura, 1997 cit în Lee și colab., 2008; Boehmer și colab., 2015; Saridakis și colab., 2016):

- Să informeze în mod explicit despre riscurile la care utilizatorii pot fi expuși atunci când utilizează internetul și TIC;
- Să identifice și conștientizeze utilizatorii cu privire la comportamentele personale de risc care pot crește vulnerabilitatea la victimizarea informatică;
- Să crească gradul de conștientizare a utilizatorilor cu privire la măsurile existente de protecție și securitate informatică, inclusiv prin informații obiective despre eficacitatea protecției disponibile;
- Să îi învețe modalități de implementare a măsurilor de protecție și securitate informatică disponibile, de ex. prin ajutor contextual și instrucțiuni pas cu pas;
- Să sublinieze rezultatele pozitive asociate cu adoptarea unui comportament online sigur.

Deși este adevărat că informațiile, promovarea strategiilor de conștientizare și educație pot fi puse în aplicare în orice grup de vârstă, practicile și inițiativele din acest domeniu s-au concentrat în principal pe copii și tineri.

Mai jos prezentăm un rezumat al unor practici universale de prevenire a criminalității informatice, care acoperă inițiative, programe și proiecte pentru copii de diferite grupe de vârstă, care se bazează pe informații, promovarea cunoștințelor și consolidarea abilităților pentru utilizarea în siguranță a internetului și a TIC .

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

Tipul de prevenție	Universal
Populația țintă	Copii cu vârsta cuprinsă între 4 și 7 ani
Teme / Probleme	Securitatea pe internet
Obiective	• Promovarea cunoștințelor, abilităților și încrederii pentru o utilizare sigură și în siguranță a internetului și a TIC; • Oferirea oportunității de învățare a principiilor / valorilor cheie pentru o utilizare sigură a internetului și a TIC: respect pentru ceilalți; consimțământ; comportament sănătos și nesănătos pe internet; căutând ajutor de la adulți de încredere.
Contextul implementării	Poate fi implementat ca grup (într-un context de clasă, de exemplu) și individual (context familial)
Descriere	• „Jessie & Friends" este un serial animat, cu trei episoade pentru copii de la 4 la 7 ani: (i) episodul 1 - 4-5 ani; (ii) episodul 2 - 5-6 ani și (iii) episodul 3 - 6-7 ani. • „Jessie & Friends" urmărește aventurile lui Jessie, Tia și Mo atunci când folosesc internetul și TIC. Personajele învață că, deși Internetul este un loc de distracție, este și un loc de risc. • Seria este însoțită de un Ghid pentru profesori, părinți și / sau îngrijitori, cu îndrumări de sesiune. • De asemenea, este completat de o carte cu povești, pentru a consolida învățarea acasă / în familie și / sau la școală
Țara de implementare	Regatul Unit
Informatii suplimentare	https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/

THINKUKNOW - "THINKUKNOW TOOLKIT"

Tipul de prevenție	Universal
Populația țintă	Tineri de 11 ani și peste
Teme / Probleme	Securitatea pe internet
Obiective	• Elaborarea de abordări sănătoase în probleme precum relațiile, sexul și internetul; • Identificarea de comportamentele negative asociate cu aceste subiecte; • Să știe unde să găsească sfaturi și îndrumări cu privire la aceste subiecte; • Să știe unde să caute ajutor atunci când sunt confruntați cu situații de risc online.
Contextul implementării	Context școlar
Descriere	Activități desfășurate: • Găsirea rapidă - joc de rol, care explorează natura „prieteniei" online, identifică riscurile și evidențiază modalități sigure de socializare online; • Tatuaj digital - discuție în perechi și în grup, introducerea tinerilor în conceptul de „tatuaj digital" (sau „amprentă digitală") și modalități de gestionare a acestuia; • Code Breaker - activitate în care tinerii încearcă să ghicească parolele definite de personaje fictive; • Thinkuknow Better? - tinerii dezvoltă sfaturi pentru a-și sprijini semenii.
Țara de implementare	Regatul Unit
Informatii suplimentare	https://www.thinkuknow.co.uk/professionals/resources/thinkuknow-toolkit/ https://www.src.ac.uk/images/news/658x300/1920/Aug19/StudAct/Thinkuknow_Toolkit.pdf

THINKUKNOW - "JOSH & SUE"

Tipul de prevenție	Universal
Populația țintă	Tinerii cu dizabilități de învățare în vârstă de 11-13 ani
Teme / Probleme	Securitatea pe internet
Obiective	• Tinerii ar trebui să poată înțelege consecințele asociate cu atitudini / comportamente necorespunzătoare online explorând comportamente de siguranță online și comportamente pozitive în relațiile interpersonale online
Contextul implementării	Contextul școlar și / sau familial
Descriere	• Filmul este disponibil în două versiuni, pentru tineri cu niveluri diferite de dizabilități de învățare. • Filmul poate fi folosit într-un context școlar și / sau familial.
Țara de implementare	Regatul Unit
Informatii suplimentare	https://www.thinkuknow.co.uk/parents/Support-tools/Films-to-watch-with-your-children/Josh_and_Sue_original1/

GHIDUL DE SIGURANTA A LUI ZUKY

Tipul de prevenție	Universal
Populația țintă	Copii (fără o vârstă specifică)
Teme / Probleme	Securitatea pe internet
Obiective	• Să informeze copiii despre riscurile de pe internet și despre strategii de securitate informatică și comportamente de protecție personală
Contextul implementării	Poate fi implementat în orice context, de către familie, îngrijitori și/sau specialiști.
Descriere	• Serie de desene animate pentru copii, unde personajul principal este „Zuky", un supererou de securitate pe internet. Această serie poate fi vizualizată pe site-ul oficial sau pe Youtube. Utilizând site-ul oficial, pe lângă videoclipuri, sunt disponibile și ghiduri și chestionare pentru copii, precum și sfaturi pentru familii și tutori legali cu privire la siguranța internetului.
Țara de implementare	Olanda
Informatii suplimentare	https://www.paloaltonetworks.com/campaigns/kids-in-cybersecurity https://www.youtube.com/channel/UCDYFyxEbTw0oF0FdzP1hlfg https://trailhead.gsnorcal.org/wp-content/uploads/2018/12/EN_PANE_0nepaper_Kids_in_Cybersecurity.pdf

PROIECT deSHAME

Tipul de prevenție	Universal
Populația țintă	Tinerii cu vârste cuprinse între 13 și 17 ani
Teme / Probleme	Hărțuire sexuală online
Obiective	• Promovarea raportării hărțuirii sexuale online[90] în rândul tinerilor • Îmbunătățirea cooperării multisectoriale în prevenirea și răspunsul la aceste comportamente
Contextul implementării	Context comunitar și școlar
Descriere	Proiectul deSHAME este finanțat de Comisia Europeană și își propune să combată hărțuirea sexuală online. Este o colaborare între Childnet (Marea Britanie), Save the Children (Danemarca), Kek Vonal (Ungaria) și UCLan (Marea Britanie). Aceasta implică dezvoltarea unei game de resurse educaționale pentru a preveni hărțuirea sexuală online și pentru a permite raportarea acesteia. În acest cadru, setul de instrumente *Step Up, Speak Up!* a fost dezvoltat - un instrument cu sesiuni practice pentru a aborda hărțuirea sexuală online în rândul tinerilor. Au fost dezvoltate, de asemenea, mai multe resurse și materiale de sprijin pentru contextul școlar.
Țara de implementare	Diferite
Informatii suplimentare	https://www.childnet.com/our-projects/project-deshame https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf

KIDS IN THE KNOW - "ZOE & MOLLY ONLINE"

Tipul de prevenție	Universal
Populația țintă	Elevi din ciclul primar
Teme / Probleme	Securitatea pe internet
Obiective	• Elevii ar trebui să poată identifica riscurile și beneficiile utilizării internetului • Elevii ar trebui să poată răspunde în siguranță la riscurile pe care le întâmpină online
Contextul implementării	Context școlar De asemenea, are un site web cu jocuri, teste și benzi desenate, care pot fi utilizate într-un context școlar, ca complement sau într-un context familial.
Descriere	• *„Zoe & Molly Online"* este o carte de benzi desenate. Dezvoltată de Centrul canadian pentru protecția copilului, proiectul „Zoe & Molly Online" este conceput pentru a promova discuțiile la clasă despre riscurile asociate schimbului de informații personale online. • Promovează implicarea și supravegherea din partea adulților, încurajând copiii să verifice întotdeauna cu un adult de încredere înainte de a partaja informații online cu oricine.
Țara de implementare	Canada
Informatii suplimentare	http://www.zoeandmolly.ca/pdfs/zm_TeacherKit_SinglePagesGr4_en.pdf https://www.zoeandmolly.ca/app/en/

[90] Proiectul definește hărțuirea sexuală online ca un set de comportamente sexuale nedorite care pot apărea pe orice platformă digitală. Acest concept cuprinde diferite forme de criminalitate cibernetică / violență abordate în partea I, capitolul 1 al acestui manual, inclusiv agresiunea cibernetică, diseminarea non-consensuală a imaginilor și videoclipurilor și diferite forme de abuz sexual și exploatare a copiilor pe internet.

4.2.1. Exemplul campaniilor de informare și sensibilizare a publicului

Mass-media sunt instrumente puternice de diseminare, jucând un rol major în prevenirea violenței și a criminalității în diferite dimensiuni (APAV, 2011).

Prin urmare, mass-media poate fi un canal important în prevenirea criminalității informatice, în special prin diseminarea informațiilor publice și a campaniilor de conștientizare în acest domeniu, fie prin diferite mijloace de comunicare, inclusiv prin internet și rețelele sociale, fie prin intermediul unor canale mai tradiționale, cum ar fi televiziunea. În orice caz, campaniile de informare și conștientizare ar trebui utilizate ca parte a unei abordări mai largi a prevenirii criminalității informatice (Brewer și colab., 2019).

Campaniile pot avea obiective diferite (Finn & Banach, 2000; Brewer și colab., 2019), cum ar fi:

- Furnizarea de informații cu privire la măsurile de securitate informatică și comportamentele personale de protecție pentru utilizarea internetului și a TIC;

IMPORTANT | PRACTICA ÎN FOCUS:

Agenția Europeană pentru Securitatea Rețelelor și Informațiilor (ENISA) promovează anual campania de conștientizare *Luna Europeană a Securității Informatice.*

Această campanie europeană urmărește să sensibilizeze amenințările privind securitatea informatică și să promoveze securitatea informatică în rândul persoanelor și organizațiilor.

Această campanie oferă, de asemenea, resurse privind protecția personală, informații despre o serie de inițiative educaționale și schimbul de bune practici.

Campaniile anterioare și resursele acestora, inclusiv videoclipuri și infografii, sunt disponibile la https://cybersecuritymonth.eu/press-campaign-toolbox/infographics

Informații complete despre inițiativa Lunii europene a securității informatice sunt disponibile la adresa https://cybersecuritymonth.eu/.

- Promovarea comportamentelor și valorilor pozitive asociate utilizării Internetului și a TIC;

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

IMPORTANT | PRACTICA ÎN FOCUS:

IMPORTANT | PRACTICA ÎN FOCUS:

În cadrul campaniei pentru *Luna europeană a securității informatice din 2019*, deviza *securitate informatică* este utilizată pentru a informa și a crește gradul de conștientizare cu privire la importanța utilizării sănătoase și sigure a TIC și a internetului în viața de zi cu zi.

Materialele campaniei pot fi accesate la: https://cybersecuritymonth.eu/#/campaign

Campania *European Cyber Security Month* și Agenția Europeană pentru Securitatea Rețelelor și Informațiilor oferă o serie de resurse de informare și promovare a conștientizării.

Printre acestea se remarcă QUIZ privind Securitatea Rețelelor și a Informației (Network and Information Security - NIS): un instrument de autodiagnosticare care permite evaluarea nivelurilor de cunoștințe și abilități pe subiecte precum securitatea informatică în general, confidențialitatea și amenințările informatice.

Acest instrument, disponibil în mai multe limbi, poate fi accesat și utilizat la: https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/

- Informarea despre comportamentele care trebuie adoptate în situații de victimizare informatică;

IMPORTANT | PRACTICA ÎN FOCUS:

IMPORTANT | PRACTICA ÎN FOCUS:

Campania de conștientizare publică *Spune Nu!* a EUROPOL își propune să sensibilizeze copiii și tinerii, astfel încât aceștia să poată identifica și acționa în legătură cu șantajul sexual online al copiilor, consolidând importanța raportării și a căutării de sprijin.

Videoclipurile campaniei (în mai multe limbi) și alte resurse de informații sunt disponibile la: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion-and-extortion-crime

- Promovarea implicării colective sau a unei părți terțe în protecția și siguranța online (de exemplu, rolul familiei în identificarea riscului asociat comportamentelor online ale copiilor lor);
- Descurajarea practicii criminalității informatice prin furnizarea de informații cu privire la riscurile asociate și consecințele negative.

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

IMPORTANT | PRACTICA ÎN FOCUS:

EUROPOL, cu un registru și un scop distinct, a lansat *Criminalitatea informatică vs. securitatea informatică: ce veți alege?* campanie de conștientizare

Disponibilă în diferite limbi, această campanie se adresează, de asemenea, tinerilor și își propune să îi descurajeze să se angajeze în criminalitatea informatică prin evidențierea consecințelor și costurilor asociate implicării în aceste comportamente ilicite.

Materialul campaniei este disponibil pentru descărcare la: https://www.europol.europa.eu/publications-documents/cyber-crime-vs-cyber-security-what-will-you-choose-poster

În cadrul inițiativei, EUROPOL oferă, de asemenea, informații și sfaturi atât pentru tineri, cât și pentru educatori și familii.

4.3. Rolul familiei în prevenție

Adulții actuali, spre deosebire de copii și tineri, nu s-au născut „nativi digitali", așa că nu acceptă atât de prompt Internetul și TIC ca ceva natural, fundamental și de necontestat în viața lor. În plus, pe lângă utilizarea lor eficientă și eficientă a internetului și a TIC fiind constrânsă de cunoștințele și abilitățile lor limitate, familia nu are adesea o conștientizare clară a activităților online ale copiilor și tinerilor lor (Richardson și Milovidov, 2019; Cross și colab. ., 2016; Lwin și colab., 2013; Öztürk & Akcan, 2016).

În mod paradoxal, adulții din familie joacă un rol cheie în informarea și educarea copiilor și tinerilor cu privire la utilizarea în siguranță a internetului și a TIC și, în consecință, în prevenirea victimizării informatice și a comportamentelor de risc online (Mesch, 2009; Notar et al. ., 2013; Morais, 2012 cit în Martins și colab., 2017; Smallbone & Wortley, 2017; Richardson și Milovidov, 2019).

Prin urmare, intervenția familiei este foarte importantă:

- În stabilirea și implementarea **regulilor cosistente** pentru utilizarea internetului și a TIC de către copii și tineri aflați în responsabilitatea adulților;
- În educarea copiilor și tinerilor cu privire la **drepturile și responsabilitățile** lor atunci când utilizează internetul și TIC;
- În **promovarea empatiei** și respectului față de ceilalți în orice context, inclusiv online;
- În furnizarea de **informații** și împuternicirea copiilor și tinerilor cu privire la probleme de confidențialitate, securitate informatică și protecție personală atunci când se utilizează internetul și TIC, precum și prezentarea clară a riscurilor asociate utilizării internetului și TIC,

inclusiv cele legate de violență și infracțiuni ;

- În **monitorizarea utilizării internetului și a TIC**, prin comunicare deschisă, învățarea utilizării internetului și a TIC și interesul pentru activitățile online de către copii și tineri aflați în responsabilitatea familiei;
- Identificarea posibililor **indicatori de victimizare informatică** (sau utilizarea nesănătoasă a TIC și a internetului) asupra copiilor și tinerilor și permiterea unei intervenții / protecții adecvate a copilului sau a tânărului în situații de criminalitate informatică;
- Menținerea **canalelor de comunicare** cu copiii și tinerii pentru a promova căutarea de sprijin / ajutor de la adulți de încredere în situații de victimizare informatică și alte circumstanțe în care protecția personală pe internet și TIC poate fi compromisă.

IMPORTANT | PRACTICA ÎN FOCUS:

INTERNETMATTERS.ORG este o organizație non-profit care își propune să împuternicească familiile să păstreze copiii și tinerii în siguranță atunci când utilizează internetul și TIC.

Platforma are informații, sfaturi și mai multe resurse specifice pentru familiile cu copii și tineri de diferite grupe de vârstă.

De asemenea, are informații despre diferite tipuri de criminalitate informatică care pot afecta copiii și tinerii, cum ar fi îngrijirea online, agresiunea informatică, furtul de identitate online, printre altele.

Platforma este disponibilă la: https://www.internetmatters.org/

PARENTINFO.ORG este, de asemenea, o platformă destinată părinților și familiilor, cu informații și sfaturi cu privire la o serie de subiecte de interes legate de internet și TIC, inclusiv probleme precum securitatea informatică, aplicațiile și tehnologia, bunăstarea și sănătatea, printre altele.

Platforma este disponibilă la: https://parentinfo.org/

În ceea ce privește rolul familiei în prevenirea criminalității informatice, conceptul de *parenting digital* a fost introdus și poate fi operaționalizat ca:

- Comunicare deschisă între familie / părinți și copii și tineri aflați în responsabilitatea lor;
- Implicarea familiei / părinților în activitățile online desfășurate de copii și tineri, în același mod în care aceștia sunt implicați în activitățile zilnice ale copiilor și tinerilor în contexte tradiționale;
- Protejarea prezenței digitale a copiilor și tinerilor, adică modul în care copilul sau tânărul se prezintă sau se descrie în activitățile lor online;
- Învățarea reciprocă între familie / părinți și copii și tineri aflați în responsabilitatea lor;
- Protejarea copiilor și tinerilor dependenți de Internet și de riscurile și amenințările TIC, în special a criminalității informatice.

4. IMPORTANȚA PREVENȚIEI ÎN COMBATEREA INFRACȚIUNILOR INFORMATICE

IMPORTANT | PRACTICA ÎN FOCUS:

Consiliul Europei a lansat *Parenting în Era Digitală. Îndrumarea părinților pentru protecția online a copiilor împotriva exploatării și abuzurilor sexuale*.

Este un ghid de bune practici pentru părinți și familii, în care sunt abordate diferite forme de abuz sexual și exploatare a copiilor prin intermediul internetului. Într-un mod practic și informativ, acest ghid împărtășește sfaturi și resurse menite să ajute părinții și familiile să protejeze copiii și tinerii de aceste fenomene și chiar să acționeze în situații în care a avut loc deja victimizarea informatică.

Ghidul este disponibil la https://rm.coe.int/digital-parenting-/16807670e8

De asemenea, Consiliul Europei pune la dispoziție o serie de alte informații și resurse educaționale privind protecția copiilor și tinerilor pe internet. De exemplu, *Manualul de alfabetizare pe internet* al Consiliului Europei, disponibil și pentru descărcare la: https://www.coe.int/en/web/children/internet-literacy-handbook.

Consultați și https://www.coe.int/en/web/children/the-digital-environment pentru informații suplimentare.

4.4. Școala ca context privilegiat de prevenire

Școala, alături de familie, este un **context de socializare foarte important** pentru dezvoltarea copiilor și tinerilor, nu numai în ceea ce privește învățarea curriculară, ci și în ceea ce privește învățarea **abilităților sociale pentru viață**. Acestea sunt abilități fundamentale pentru funcționarea și comportamentul copilului sau tânărului în raport cu lumea din jur (Saavedra & Machado, 2010), în special în contextele lor relaționale cele mai apropiate, cum ar fi grupul de semeni și familia, dar și în funcționarea lor în societate. Calitatea legăturii dintre copil sau tânăr și școală este, de asemenea, un factor de protecție împotriva comportamentelor de risc, motiv pentru care este deosebit de important să promovăm oportunități, în context școlar, pentru întărirea bunăstării și a relațiilor pozitive ale copiilor și tineri cu colegii lor și specialiștii din educație (McNeely, Nonnemaker și Blum, 2002 cit în Saavedra & Machado 2010).

Școala este astfel un context natural pentru implementarea inițiativelor de prevenire a criminalității și violenței, deoarece majoritatea copiilor frecventează școala și „trăiesc" în acest context o parte semnificativă a timpului lor (Durlak, 1995 cit in idem).

Tabelul de mai jos prezintă un set de caracteristici dezirabile pentru eficacitatea programelor de prevenire în contextul școlii (APAV, 2011; Brewer și colab., 2019):

Tabel 8: Principalele aspecte care trebuie luate în considerare în programele de prevenire la școală

Baza teoretică coerentă: punctul de plecare pentru planificare ar trebui să fie o bază teoretică clară, cu dovezi ale succesului oferite de cercetare.

Abordare ecologică: programul ar trebui să se concentreze nu numai pe individ, ci și pe contextele sociale ale acestuia: familie, școală, comunitate. Programele de intervenție școlară au cel mai mare succes atunci când sunt completate de intervenții familiale și comunitare, deoarece acestea pot întări și promova schimbarea comportamentului.

Abordare integrată a factorilor de risc și de protecție: programele ar trebui dezvoltate într-un mod care să reducă factorii de risc și să promoveze factorii de protecție.

Atenție individualizată: intervenția trebuie planificată în funcție de nevoile specifice ale individului / grupului; programele ar trebui să fie adecvate vârstei, nivelului de dezvoltare și caracteristicilor grupurilor țintă.

Intervenție precoce și adaptată la dezvoltare: intervenția ar trebui să aibă loc cât mai devreme posibil, în funcție de nivelul de dezvoltare al indivizilor.

Alegerea țintelor potrivite pentru schimbare: creșterea cunoștințelor, schimbarea atitudinilor, schimbarea comportamentelor și învățarea de noi abilități sunt cele mai comune obiective pentru schimbare.

Implicarea colegilor: dată fiind influența colegilor, există programe de prevenire bazate pe acțiunea grupurilor de colegi ca agenți preventivi.

Utilizarea metodelor interactive de transmitere a informațiilor: activitățile ar trebui desfășurate într-un format interactiv, atrăgător și adecvat vârstei: grupuri de discuții, dezbateri, brainstorming, joc de rol etc.

Învățarea sistematică și formarea abilităților: ar trebui oferite oportunități pentru formarea abilităților sociale: rezolvarea conflictelor, asertivitatea, luarea deciziilor, ascultarea activă, precum și instruirea prin strategii cognitiv-comportamentale, cum ar fi jocul de rol, simularea unor situații apropiate de realitate și experiențele personale ale participanților etc.

Promovarea conștiinței sociale: programele de prevenire ar trebui să îi ajute pe destinatari să înțeleagă emoțiile și gândurile altora (empatie) și să aprecieze interacțiunea pozitivă cu diferite grupuri.

Managementul emoțional: programele de prevenire ar trebui să ajute participanții să se ocupe în mod adecvat și eficient de emoții (autogestionare emoțională).

Concentrați-vă pe relații: programele de prevenire ar trebui să pregătească participanții pentru a stabili relații pozitive cu ceilalți, promovându-le capacitatea de a comunica, de a coopera, de a negocia soluții la conflicte, de a căuta ajutor (dacă este necesar) și de a rezista presiunii colegilor și provocărilor de mediu într-un mod adecvat.

Pregătirea, supravegherea și munca multidisciplinară: pregătirea profesioniștilor este fundamentală pentru o implementare de calitate și de succes.

Abordare neutră de gen: este important să se respecte identitatea de gen a destinatarilor și să se ia în considerare această variabilă în procesul de intervenție.

Concentrați-vă asupra nivelurilor normative ale problemelor: în afară de cele mai grave sau grave forme de violență, programele de prevenire ar trebui să abordeze nivelurile „normative" de violență (inclusiv forme subtile de violență care sunt de obicei tolerate sau normalizate de grupul țintă al intervenției).

Alternative comportamentale: intervenția ar trebui să prezinte alternative comportamentale care sunt incompatibile cu utilizarea unui comportament inadecvat.

Informații: programele ar trebui să acopere și furnizarea de informații despre factorii de risc și consecințele anumitor comportamente și despre structurile de sprijin social.

Conținut clar și materiale simple: programul ar trebui să aibă ghiduri și / sau manuale ușor de utilizat pentru a sprijini implementarea.

Implementarea integrală a programului: programele trebuie să fie puse în aplicare în întregime și să îndeplinească obiectivele propuse, cu mecanisme de monitorizare a implementării acestora.

Intervenție intensivă și pe termen lung: programele de prevenire trebuie să fie intensive și pe termen lung.

Evaluare: programele de prevenire ar trebui să includă măsurarea independentă (externă echipei responsabile de crearea / implementarea lor) a modificărilor realizate în grupurile țintă utilizând metodologii validate.

Sustenabilitate: este, de asemenea, important să se evalueze costurile versus beneficiile implementării și sustenabilitatea lor pe termen lung.

IMPORTANT | PRACTICA ÎN FOCUS:

NoTrap! este un program italian de intervenție online și școlar conceput pentru prevenirea și combaterea agresiunii și a agresiunii informatice.

TIC este punctul de plecare al programului, cu două ipoteze de bază:

- Utilizarea TIC poate crește riscul de intimidare informatică.
- TIC poate fi, de asemenea, utilizat ca instrument de formare și consolidare a cunoștințelor și abilităților în prevenire și acțiune împotriva agresiunii informatice.

Studiile de evaluare ale acestui program au identificat rezultate pozitive în reducerea agresiunii și a agresiunii informatice (Palladino și colab., 2016).

IMPORTANT | PRACTICA ÎN FOCUS:

Proiectul *CyberTraining: Un manual de formare bazat pe cercetare privind hărțuirea informatică* s-a concentrat pe problema hărțuirii informatice, cu sprijinul echipelor de cercetare din Germania (responsabile de coordonare), Portugalia, Spania, Marea Britanie, Irlanda și experții în tehnologiile informației și comunicării și experții în cultură digitală din Bulgaria, Elveția și Norvegia.

Acest proiect a realizat un manual de instruire cu privire la hărțuirea informatică, destinat în special specialiștilor care lucrează în acest domeniu cu publicuri țintă diferite, în special tineri, familii și școli. Pe lângă includerea unei componente teoretice, acest manual oferă și îndrumări, suport și resurse care pot fi utilizate pentru prevenirea și combaterea acestei probleme (Matos și colab., 2011).

4.5. Prevenția pentru grupurile vulnerabile: cazul copiilor și tinerilor

În calitate de nativi TIC, copiii și tinerii prezintă **un interes și un apetit aproape natural pentru activități online**. Acest lucru este avantajos în multe domenii, dar crește, de asemenea, **vulnerabilitatea acestui grup la implicarea în criminalitatea informatică**, atât în ceea ce privește victimizarea informatică, cât și comiterea faptei (Alkan & Citak, 2007 cit în Edirisuriya & Liyanage, 2016).

Pentru acest grup, comunicarea prin intermediul instrumentelor de comunicare acceptate de Internet și a comunităților virtuale nu sunt subculturi tehnologice, ci mai degrabă modalități de a păstra legătura cu colegii. Comunicarea prin aceste mijloace de informare pare a fi privilegiată de această populație, deoarece oferă un sentiment mai mare de confidențialitate și anonimat, favorizând dezinhibarea, în detrimentul comunicării față în față (Chisholm, 2014).

Deoarece se mișcă în mod natural prin Internet și TIC, nu este neobișnuit ca tinerii să fie implicați în activități ilegale online, fie căutând senzații tari, pentru distracție sau pentru că nu asociază posibile consecințe negative cu comportamentul lor. PRACTICA ÎN FOCUS rezumată mai sus - *Criminalitatea informatică vs securitatea informatică: Ce veți alege?* a EUROPOL, o campanie de conștientizare - informează și avertizează cu privire la consecințele implicării în activități online ilicite și, în opoziție, încearcă să promoveze adoptarea de comportamente pozitive și normative.

În mod similar, riscul de victimizare informatică este, de asemenea, mai mare în rândul populației mai tinere. Vezi STATISTICILE ÎN FOCUS prezentate în diferite puncte din partea I, capitolul 1 al acestui manual.

IMPORTANT | PRACTICA ÎN FOCUS:

În urma campaniei de conștientizare publică a EUROPOL privind șantajul sexual online menționată mai sus, campania *VIAȚA TA ESTE ONLINE. PROTEJEAZ-O!* oferă o serie de informații pentru tineri care vizează reducerea riscului asociat comportamentului lor online și a nivelurilor de expunere.

Acoperă informații despre măsurile de securitate informatică care urmează să fie adoptate și care măresc **nivelurile de confidențialitate digitală**, în special pe rețelele sociale, și abordează și alte **comportamente de protecție personală** care reduc riscul victimizării informatice.

Consultați https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media.

În plus, *VIAȚA TA ESTE ONLINE. PROTEJEAZ-O!* oferă, de asemenea, informații și instrucțiuni despre cum să acționăm în situații de victimizare informatică, cum ar fi:

- Cum să solicitați eliminarea conținutului de pe diferite platforme în cazul divulgării non-consensuale a imaginilor și videoclipurilor: https://www.europol.europa.eu/removing-links-to-explicit-content
- Cum să cereți ajutor și să raportați situațiile de victimizare informatică: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/are-you-victim-get-help-report-it-we-are-here

4.6. Prevenirea criminalității informatice situaționale: o chestiune de oportunitate

Prevenirea criminalității informatice situaționale este o paradigmă teoretică care se concentrează pe circumstanțele asociate oportunităților criminale și modul în care mediul, condițiile și contextul pot fi modificate pentru a preveni aceste oportunități criminale. Această paradigmă este asociată cu teoria alegerii raționale[91] și teoria activității de rutină (Hinduja și Kooi, 2013):

- Alegerea rațională funcționează la un nivel micro și presupune că comportamentul criminal este condus de un scop care ar duce la un beneficiu. Astfel, eventualele schimbări în structura oportunității pot afecta percepțiile de risc, efort și recompensă.
- Activitățile de rutină funcționează la nivel macro, demonstrând că schimbările din viața de zi cu zi afectează mișcarea țintelor probabile ale infracțiunilor, probabilitatea de acțiune a eventualilor infractori și nivelurile de supraveghere.

Prevenirea situației criminalității introduce potențialul de schimbare în mediile în care poate apărea criminalitatea, făcând aceste medii mai puțin atractive pentru infractorii motivați. Prevenirea criminalității se bazează astfel pe reducerea oportunităților infractorilor de a beneficia de vulnerabilități prin gestionarea, proiectarea și manipularea acelui mediu, adică prin **crearea de obstacole în mediu care reduc probabilitatea oportunităților infracționale**. În mod ideal, aceste eforturi vor servi la **creșterea riscului și a efortului** asociat cu activitatea ilicită și la **diminuarea recompenselor unei infracțiuni de succes**. Dacă prezența și atractivitatea oportunităților criminale sunt reduse, atunci rezultatul va fi o reducere a criminalității (Clarke, 1997, citită în Hinduja și Kooi, 2013).

De-a lungul mai multor decenii, o serie de propuneri și măsuri specifice de intervenție au fost definite pentru mediile în care apar infracțiuni - acestea se numesc **tehnici de prevenire a situației**. Obiectivul lor principal este de a reduce posibilitatea ca infracțiunile să apară prin schimbarea condițiilor de mediu. Există cinci categorii de prevenire situațională și, în fiecare dintre aceste categorii, pot fi aplicate cinci tehnici specifice (Cornish & Clarke, 2003 cit în Agustina, 2015):

Categorie *Creșteți efortul*:

Dacă efortul de a comite o anumită infracțiune trebuie să crească, ar putea fi posibil să se descurajeze făptuitorul de la comiterea acesteia.

Această categorie include 5 tipuri de tehnici:

- îngreunarea țintei (implementarea barierelor care îngreunează accesul la țintă);
- controlul accesului la facilități (blocarea accesului la locurile în care pot apărea acțiuni penale);
- controlarea ieșirilor (controlarea ieșirilor / mișcărilor într-un loc);

[91] Teoriile criminologice (și aplicarea lor la înțelegerea criminalității informatice) sunt abordate în partea I, capitolul 3, secțiunea 3.1 din acest manual.

- deviază infractorii (schimbă tiparele de mișcare ale potențialilor făptași)
- instrumente de control (limitarea accesului la instrumentele care fac parte din *modus operandi*).

Categorie *Creșteți riscurile*:

Aceste tehnici sunt menite să crească riscul detectării făptuitorului și includ:

- activități de protecție sporite / pază extinse (crearea de activități astfel încât oamenii să se simtă mai protejați; de exemplu, supravegherea cartierului);
- asistarea supravegherii naturale (de exemplu, prin creșterea vizibilității unei anumite locații);
- reducerea anonimatului;
- supravegherea informală (de exemplu, prin deplasarea sporită a personalului într-o zonă comercială);
- supravegherea formală (de exemplu, prin poliție sporită)

Categorie *Reduceți recompensele*:

Această categorie are ca scop reducerea recompenselor de care pot beneficia infractorii potențiali atunci când comit o infracțiune.

Principalele tehnici sunt:

- ascunderea țintelor (de exemplu, parcarea într-un garaj privat, mai degrabă decât într-un loc public / stradă);
- îndepărtarea țintelor (de exemplu, scoaterea dispozitivelor electronice și a altor bunuri la parcarea mașinii);
- identificarea proprietății (de exemplu, înmatricularea vehiculului);
- perturbarea tranzacțiilor de pe piață (de exemplu, acordarea de licențe pentru servicii și tranzacții);
- refuzarea beneficiilor (de exemplu, utilizarea unei parole pentru telefonul mobil).

Categorie *Reduceți provocarea*:

Această categorie are ca scop prevenirea declanșatorilor de practică criminală.

Principalele tehnici sunt:

- reducerea frustrărilor și a stresului (de exemplu, informarea despre sosirea / timpul de așteptare al transportului public);
- vitarea disputelor (de exemplu, separarea suporterilor sportivi în meciurile de fotbal / sport);
- reducerea excitației emoționale (de exemplu, controlul vizionării violenței în mass-media);
- neutralizarea presiunii colegilor (de exemplu, campaniile de conștientizare);

- descurajarea imitației (de exemplu, menținerea spațiilor curate și îndepărtarea rapidă a indicatorilor de vandalism).

Categorie *Eliminați scuzele*:

Include următoarele tehnici de prevenire a situației:

- stabilirea de reguli;
- afișarea de instrucțiuni (de exemplu, semne precum „fără parcare");
- conștiința alertă (de exemplu, conștientizarea comportamentului ilegal);
- să asiste conformarea (de exemplu, la evenimente festive, să faciliteze accesul la transportul public);
- controlarea alcoolului și drogurilor (de exemplu, impunerea unui număr maxim de băuturi în localurile de noapte).

Abordările de prevenire a situației au fost utilizate pe scară largă în contexte *tradiționale* și s-au dovedit utile în reducerea diferitelor tipuri de infracțiuni *tradiționale*. A fost de asemenea analizată relevanța prevenirii situației în combaterea criminalității informatice (Brewer și colab., 2019).

În acest context, Miró Llinares (2012, cit în Agustina, 2015) a prezentat o combinație **de măsuri concrete de prevenire a criminalității informatice**:

Tabel 9: Tehnici de prevenire a situației aplicate criminalității informatice

Reducerea mediului de incidență	Creșterea efortului perceput	Creșterea riscului perceput	Reducerea recompenselor percepute	Eliminarea scuzelor
Nu introduceți ținte	Controlați accesul la sistem	Extindeți tutela / supraveghere	Ascundeți ținte	Stabiliți reguli
Identificați zonele de risc	Detectați și împiedicați atacul	Reduceți anonimatul	Eliminați țintele	Setați reguli
Decontaminați / curățați reziduurile	Deflectați infractorii	Întăriți supravegherea formală	Eliminați beneficiile	Întăriți conștiința morală
Separați țintele	Controlați instrumentele / armele	Sprijiniți supravegherea naturală	Perturbați piețele	Asistați conformarea

Au fost dezvoltate cinci categorii - reducerea mediului de incidență; creșterea efortului perceput; creșterea riscului perceput; reducerea recompenselor percepute; eliminarea scuzelor - și acestea

includ 20 de tehnici situaționale de prevenire a criminalității informatice. Reducerea mediului de incidență include neintroducerea țintelor (de exemplu, fără acces la chat-uri), identificarea zonelor de risc (de exemplu, campanii de informare privind riscul pe rețelele sociale), decontaminarea / curățarea reziduurilor și separarea țintelor (de exemplu, crearea de subrețele locale de securitate). Creșterea efortului perceput include: controlul accesului la sistem (de exemplu, actualizarea sistemelor de operare și a parolelor și licențelor); detectarea și prevenirea atacurilor (de exemplu, antivirus; anti-spyware; anti-spam); devierea infractorilor (de exemplu, eliminarea conținutului ilegal; refuzul accesului[92] la anumite adrese IP); controlul instrumentelor / armelor. Creșterea riscului perceput acoperă extinderea tutelei / supravegherii (de exemplu, raportarea din partea unor terți), reducerea anonimatului (de exemplu, identificarea adreselor IP; înregistrarea pe forumurile web; sistemele de identificare a utilizatorilor), consolidarea supravegherii formale (de exemplu, echipe specializate în investigarea criminalității informatice) și asistarea supravegherii naturale (de ex. îmbunătățirea sistemelor de identificare IP). A patra categorie se concentrează pe: ascunderea țintelor (de exemplu, utilizarea sistemelor de criptare; ascunderea datelor personale în rețelele sociale); eliminarea țintelor (de exemplu, utilizarea hard disk-urilor amovibile; alegerea sistemelor de plată alternative, cum ar fi PayPal; neacceptarea mesajelor de la persoane necunoscute); eliminarea beneficiilor; perturbarea piețelor (de exemplu, controlul site-urilor web cu descărcare directă). În cele din urmă, eliminarea scuzelor include: stabilirea regulilor (de exemplu, armonizarea juridică internațională); stabilirea regulilor (de exemplu, notificări de confidențialitate pe rețelele sociale); consolidarea conștiinței morale (de exemplu, creșterea gradului de conștientizare pentru proprietatea intelectuală); și asistarea conformității (de exemplu, concursuri legale de hackeri; software deschis mai puternic).

Dovezile disponibile cu privire la eficacitatea tehnicilor de prevenire a situației pentru criminalitatea informatică s-au concentrat pe creșterea efortului, cum ar fi mecanismele/ software de control și detectare și pe creșterea riscului prin instrumente formale de supraveghere. De exemplu, cercetările privind eficacitatea produselor antivirus în detectarea și prevenirea infecțiilor malware arată că majoritatea produselor sunt eficiente în detectarea și prevenirea acestor infecții (Brewer și colab., 2019).

[92] IP se referă la adresa protocolului de internet și se referă la eticheta / codul atribuit fiecărui dispozitiv conectat la rețeaua computerului.

BIBLIOGRAFIE
WEBOGRAFIE

BIBLIOGRAFIE
WEBOGRAFIE

BIBLIOGRAFIE

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.

BIBLIOGRAFIE

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.

BIBLIOGRAFIE

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.

BIBLIOGRAFIE

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).

WEBOGRAFIE

https://dre.pt/legislacao-consolidada/-/lc/34520775/view

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis

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

https://www.kaspersky.com/blog/online-dating-report/

https://www.cncs.gov.pt/recursos/glossario/

https://www.innocentlivesfoundation.org/gaming-and-grooming-how-minecraft-and-fortnite-could-be-dangerous/

https://articles.forensicfocus.com/2019/12/17/investigating-nonconsensual-intimate-image-sharing/

https://apav.pt/cibercrime/

https://techterms.com/definition/hardware

https://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-COR-1-DCL-1/en/pdf

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://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf

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:
978-989-53116-2-0