Manual ROAR

–

da compreensão e prevenção do cibercrime
ao apoio e empoderamento das vítimas

ROAR
empoderamento às vítimas de cibercrime

APAV
associação portuguesa de apoio à vítima

Este manual foi financiado pelo Fundo para a Segurança Interna – Polícia da União Europeia

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

Parceiros:
Ministério da Administração Interna (MAI) | Portugal
Procuradoria-Geral da República (PGR) | Portugal
PT Portugal | Portugal
Weisser Ring | Alemanha
ACTEDO | Roménia

ISBN: 978-989-54855-3-6
Depósito Legal:

Título:
Manual ROAR - Da compreensão e prevenção do cibercrime
ao apoio e empoderamento das vítimas

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

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

ÍNDICE

ÍNDICE

PARTE I
COMPREENDER

PARTE I

COMPREENDER

1. CIBERCRIME: UMA ABORDAGEM À SUA CONCETUALIZAÇÃO

1.1. As tecnologias de informação e comunicação [TIC] e a emergência do cibercrime

DESTAQUE | ESTATÍSTICAS EM FOCO:

Segundo o EUROSTAT[1], em 2017, 87% das unidades residenciais na União Europeia possuíam acesso à Internet, ao passo que os dados de 2010 apontavam para uma proporção de 70%.

Mais de 85% das pessoas inquiridas referiram utilizar diariamente a Internet. As taxas mais elevadas de utilização foram identificadas na Itália, na Dinamarca, em Malta, na Holanda e na Suécia.

O EUROSTAT analisou também a utilização da Internet por parte das empresas e organizações: apenas 3% dos negócios na União Europeia não possuíam Internet em 2017, sendo que as maiores proporções de não utilização foram encontradas na Roménia e na Grécia.

No mesmo inquérito, o EUROSTAT aferiu alguns indicadores de comércio eletrónico (*e-commerce*[2]): nos últimos 10 anos, a realização de compras *online* aumentou para utilizadores/as de Internet de todas as idades, com particular destaque para jovens entre os 16 e os 24 anos. Também na auscultação de empresas e organizações, foi possível identificar que a dimensão de negócios que realizam *e-commerce* era, em 2017, de 20%.

Os dados supra (e muitos outros que também o confirmam) dão conta da crescente utilização da Internet, incluindo na União Europeia, aos mais diversos níveis. Vêm ainda reiterar que a Internet é, de facto e cada vez mais, global, instantânea, intrinsecamente transfronteiriça, fornecendo uma estrutura de rede descentralizada e permitindo a representação digital de informação (Koops, 2010).

A Internet e as Tecnologias de Informação e Comunicação (TIC)[3] vieram também providenciar, por conta dessas mesmas características, oportunidades variadas para a prática de crimes, modificando e exponenciando as possibilidades de ocorrência da criminalidade, seja porque se constituem em si mesmo enquanto alvos potenciais do crime, mas também porque podem fornecer os meios ou ferramentas através dos quais outros crimes podem ser cometidos (van Wilsem, 2011).

Poderá, portanto, afirmar-se que a Internet veio proporcionar **novas formas e oportunidades de praticar ou cometer crimes que poderemos designar como "convencionais"**, como a perseguição, o abuso sexual de crianças ou a burla, mas veio igualmente alavancar o **surgimento de novas formas de criminalidade**, desta feita exclusivamente associadas ao uso de computadores, das TIC e dos sistemas informáticos, tais como o *hacking*, o DDoS e o *malware*, que serão detalhados em campos seguintes deste Manual (Yucedal, 2010; Jahankhani, Al-Nemrat & Hosseinian-Far, 2014).

Em maior detalhe, os recursos proporcionados pela Internet, designados de chaves transformadoras[4], vieram **revolucionar o modo como a criminalidade pode ser praticada** (Wall, 2007 *cit in* Jahankhani et al., 2014). Referimo-nos, em concreto, às seguintes características promovidas ou precipitadas pela Internet:

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

2 A *world wide web* permite que pessoas de todo o mundo se envolvam em atividades comerciais, sem limites temporais e espaciais. O termo *e-commerce*, em Português, comércio eletrónico, pode ser definido como uma ferramenta de estatística para calcular as transações de bens e serviços na Internet ou como um sistema de informação que fornece catálogos de produtos na Internet (Poong, Zaman & Talha, 2006).

[3] Tecnologias de Informação e Comunicação (TIC) dizem respeito a todos os meios técnicos utilizados para tratar informação e auxiliar a comunicação, incluindo *hardware* de computador e redes e *software*.

[4] Traduzido da expressão *tranformative keys*.

- **Globalização**: o ciberespaço oferece novas oportunidades para exceder os limites convencionais;
- **Redes distribuídas**: geram novas oportunidades para a vitimação;
- **Sinopticismo e panopticismo**: fortalecem a capacidade para vigiar potenciais vítimas;
- **Trilhas de dados**: criam novas oportunidades para cometer cibercrimes.

Mais ainda, a Internet conduziu ao surgimento de um conjunto de contextos online nos quais o cibercrime poderá ter lugar. São eles:

- A ***surface web*** (*websites* e computadores acessíveis e com ligação à Internet);
- A ***deep web*** (*websites* não pesquisáveis na *surface web*; *intranets* e bases de dados médicas);
- A ***dark web*** (subtipo de *deep web* que constitui uma plataforma atrativa para a prática e preparação de atividades ilegais).

(Maimon & Louderback, 2019).

Neste "ecossistema", poderemos identificar a interação dos seguintes agentes ou intervenientes, cujo respetivo comportamento possibilita a ocorrência do cibercrime:

- **Cibercriminoso/a**;
- **Facilitadores**[5] – aquele(s) que apoiam a realização do cibercrime, como programadores e *coders*[6] que desenvolvem *software*[7] malicioso (*malware*[8]), distribuidores e fornecedores que vendem/fornecem esse tipo de ferramentas que permitem a prática de cibercrime.
- **Alvos**;
- **Guardiões** – autoridades policiais e administradores de sistemas.

1.2. Das definições de cibercrime às tipologias

Procuraremos, nesta secção do Manual, apresentar definições possíveis para o conceito de cibercrime, recorrendo também, para a melhor compreensão deste fenómeno, a diferentes tipologias e categorizações, como meio de demonstrar a sua complexidade e a miríade de formas ou tipos de atos contemplados.

O **conceito de cibercrime** surgiu inicialmente através da designação "crime informático", correspondendo a todos os crimes que usam computadores ou outros dispositivos análogos, incluindo redes e outros meios de acesso. Referiam-se, por isso mesmo, a todo o tipo de **ataques contra a disponibilidade, integridade e confidencialidade de sistemas informáticos, sistemas de informação e recursos que os suportam** (*hardware*[9]) (Gouveia, 2016 *cit in* Maia, Nunes, Caridade, Sani, Estrada, Nogueira, Fernandes & Afonso, 2016).

A crescente utilização da Internet e das TIC precipitou o surgimento de outros crimes informáticos que se estendem para além do já citado ataque contra a disponibilidade, integridade e confidencialidade de sistemas informáticos.

[5] Traduzido do conceito *enablers*.

[6] *Coders* são indivíduos que se dedicam à produção de código, à sua testagem e colocação em servidor para execução.

[7] *Software* diz respeito a sequências de instruções abstratas de um programa, que descrevem cálculos a serem executados num dispositivo de computação (Councill & Heineman, 2001).

[8] *Malware* é *software* malicioso destinado a infiltrar-se, de forma ilícita, em sistemas de computadores alheios, com o intuito de causar danos, alterações e/ou aceder indevidamente a informação/dados (confidenciais ou não).

[9] As partes internas de *hardware* de um computador são geralmente denominadas de componentes (discos rígidos e RAM), enquanto os dispositivos externos de *hardware* são geralmente designados por periféricos (monitores, teclados, impressoras e *scanners*).

1. CIBERCRIME: UMA ABORDAGEM À SUA CONCETUALIZAÇÃO

Surge, assim, a adoção de conceitos similares ao de criminalidade informática, como *cibercrime*, *e-crime*, *crime digital* e *crime eletrónico*.

Nessa perspetiva, desde logo mais abrangente, o cibercrime pode ser também definido como **um crime em que a rede de computadores é um *alvo* ou uma *ferramenta* substancial** (Koops, 2010). Observando a definição da Comissão Europeia (2007)[10], o cibercrime inclui os crimes cometidos usando redes de comunicação eletrónicas e sistemas de informação e os crimes contra essas redes e sistemas.

Atendendo à natureza da cibercriminalidade e à complexidade deste conceito, vários são os/as autores/as que propõem tipologias ou categorizações, tendo em vista uma melhor compreensão acerca do seu âmbito, abrangência e multiplicidade de fenómenos associados.

O cibercrime pode, assim, ser categorizado em:

- **Crimes ciber-dependentes**[11] - estão associados a novas formas de criminalidade, cuja ocorrência depende da existência e da utilização das TIC, de computadores e de redes de computadores (Leukfeldt, Notté & Malsch, 2020; Maimon & Louderback, 2019).

- **Crimes possibilitados pela Internet e pelas TIC**[12] - formas tradicionais de criminalidade nas quais as TIC desempenham um papel importante para a sua prática, incluindo crimes com motivação financeira, mas também formas de violência interpessoal e crimes sexuais. Alguns exemplos são o *ciber-stalking* ou as burlas cometidas através da Internet (Leukfeldt et al., 2020), que abordaremos em seguida.

Esta categorização da cibercriminalidade distingue a criminalidade ciber-dependente da criminalidade possibilitada pela Internet e pelas TIC. No entanto, neste último caso, as diferentes formas de cibercriminalidade que são possibilitadas ou ativadas pela Internet e pelas TIC podem ainda, por sua vez, ser subdivididas em:

- Cibercrimes financeiramente motivados (e.g., *phishing*[13] e *romance scams*[14]);
- Cibercrimes em relacionamentos interpessoais (e.g., *ciber-stalking*);
- Cibercrimes sexuais (e.g., *revenge porn*[15]).

À categorização anterior, poderão adicionar-se outras, como as sintetizadas no quadro seguinte.

[10] Veja-se Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões: *Rumo a uma política geral de luta contra o cibercrime* , disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM%3Al14560.

[11] Traduzido da expressão *cyber-dependent* crimes.

[12] Traduzido da expressão *cyber-enabled* crimes.

[13] Informação adicional sobre este fenómeno no ponto 1.3 da Parte I deste Manual.

[14] Informação adicional sobre este fenómeno no ponto 1.3 da Parte I deste Manual.

[15] Informação adicional sobre este fenómeno no ponto 1.3 da Parte I deste Manual.

1. CIBERCRIME: UMA ABORDAGEM À SUA CONCETUALIZAÇÃO

Quadro I-1: Tipologias e Categorizações de Cibercriminalidade

Wall, 2005 *cit in* Reep-van den Bergh & Junger, 2018	**Crimes contra computadores**: implicam o acesso não autorizado aos limites dos sistemas dos computadores, como *hacking/cracking*[16], em que os computadores são o foco/alvo do ataque [e.g., vírus informáticos]; **Crimes ao usar computadores**: em que as TIC são utilizadas para a prática do crime [e.g., furto de identidade e uso de cartões de crédito falsos *online*]; **Crimes nos computadores**, nos quais o conteúdo criminal é o crime [e.g., material de abuso e/ou de exploração sexual de crianças *online*, ameaças de violência e terrorismo].
Jahankhani et al., 2014	**Computador como alvo**: furto de propriedade, acesso ilícito a informações [e.g., lista de clientes] e sua utilização para obtenção de outros benefícios, nomeadamente financeiros, através de ameaça, por exemplo; **Computador como instrumento do crime**: uso fraudulento de informações sobre cartões e contas bancárias, conversão ou transferência de contas, burlas com cartões de crédito, por exemplo; **Computador incidental a outros crimes**: lavagem de dinheiro e transações bancárias ilegais, por exemplo; **Crime associado à prevalência de computadores**: pirataria de *software*, violação de direitos autorais de programas, falsificação de equipamentos/programas e roubo de equipamento tecnológico.
Yar, 2006 *cit in* Jahankhani et al., 2014	**Invasão ou trespasse**[17]: cruzamento de fronteiras virtuais dos sistemas informáticos, causando danos aos direitos de propriedade ou titularidade [e.g., *hacking*]; **Engano e furto**[18]: uso fraudulento de cartões de crédito e dinheiro, através de invasão de contas bancárias *online* e do *e-banking*; **Material de abuso e/ou de exploração sexual de crianças *online***[19]; **Violência *online***, na qual se incluem a perseguição/assédio persistente online [*ciber-stalking*] e o discurso de ódio *online*; **Crimes contra o Estado**, nas quais se incluem atividades *online* que violam leis que protegem a integridade do Estado, como o terrorismo, espionagem e divulgação de segredos oficiais.

DESTAQUE | INFORMAÇÃO EM FOCO:

Não obstante estas e outras categorizações, não existe uma concetualização universal dos diferentes tipos de cibercrime. Das tipologias anteriores depreende-se, *grosso modo*, que a cibercriminalidade pode organizar-se em:

- Cibercriminalidade contra computadores e sistemas informáticos;
- Cibercriminalidade facilitada ou praticada por intermédio de computadores e sistemas informáticos.

Depreende-se igualmente que, na abordagem à temática do cibercrime, nos referimos, na verdade, a um **conjunto de crimes diversos** que envolvem sistemas informáticos e computadores enquanto instrumentos para a prática do crime ou enquanto alvos.

[16] Informação adicional sobre este fenómeno no ponto 1.3 da Parte I deste Manual.

[17] Traduzido da expressão *cyber-trespass*.

[18] Traduzido da expressão *cyber-deceptions and theft*.

[19] Traduzido da expressão *cyber-pornography*.

1.3. Os diferentes tipos de cibercrime: tendências atuais

Nas secções seguintes deste Manual, apresentamos um breve enquadramento relativo àqueles que atualmente são considerados os principiais fenómenos (ou, pelo menos, os fenómenos que merecem maior destaque ou preocupação) em matéria de cibercriminalidade. Ressalva-se, no entanto, que o cibercrime e as suas diversas formas de expressão, inclusivamente pelos contextos em que ocorrem, pelas ferramentas que utilizam e/ou pelos alvos aos quais se dirigem, estão em mutação constante, sendo possível a inclusão de outros tipos de cibercrime não contemplados neste ponto do Manual.

Importa igualmente salientar que, apesar do crescente conhecimento relativamente aos diversos fenómenos de cibercriminalidade, ainda é insipiente a informação acerca da real dimensão da vitimação pelos diferentes tipos de cibercrimes, desconhecendo-se, portanto, quais as proporções reais da sua prevalência na população (Reep-van den Bergh & Junger, 2018). Com efeito, sempre que possível, ao longo das secções seguintes, são disponibilizados dados provenientes de estatística oficial de cibercriminalidade reportada, de inquéritos de vitimação criminal e/ou de outros estudos que possibilitam, de algum modo, mensurar a dimensão dos diferentes tipos de cibercrime, nomeadamente a nível europeu.

DESTAQUE | ESTATÍSTICAS EM FOCO:

O estudo de Reep-van den Bergh e Junger (2018) procurou, através da análise a diferentes inquéritos de vitimação, encontrar uma estimativa aproximada da prevalência do cibercrime na Europa.

Alguns do principais resultados encontrados são seguidamente sintetizados:

- Entre 0,6% e 3,5% da população relatou ter sido vítima de **burla no comércio eletrónico** e, de entre as situações de cibervitimação identificadas, aproximadamente, 90% diziam respeito à aquisição de bens ou serviços pagos, muito embora não recebidos.
- As taxas de prevalência de **burlas com cartões de crédito/pagamentos *online*** variam entre 0,4% e 2,2%.
- Cerca de 3% da população referiu ter sido vítima de alguma forma de ***ciber-bullying***, incluindo comportamentos de ameaça, com um proporção que varia entre 0,6% e 1,0%, e de assédio, em proporções semelhantes às anteriores (0,7% a 1,1%).
- No que ao cibercrime diz respeito, pese embora os intervalos de variação, o ***hacking*** e o ***malware*** foram identificados enquanto formas de cibervitimação com prevalência mais expressiva: entre 1,2% e 5,8% da população referiu ser vítima de *hacking* e entre 2% a 15% indicou ter sido alvo de *malware*.

O estudo completo está disponível em: Reep-van den Bergh, C. M., & Junger, M. (2018). Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, 7: 1-15.

Os tipos de cibercrime acima indicados, bem como outros, serão abordados em seguida.

Todavia, importa também contextualizar as fragilidades associadas à medição da cibercriminalidade, desde o desconhecimento generalizado da população em geral face às diferentes formas de cibercrime, o poderá levar a uma subestimação do cibercrime efetivamente experienciado e reportado às autoridades, à desvalorização de alguns dos fenómenos de cibercrime, entre outros aspetos que comprometem o conhecimento da dimensão real da cibercriminalidade (Maimon & Louderback, 2019).

1.3.1. *Hacking e Cracking*

Hacking ou ***cracking*** são habitualmente definidos como o **acesso não autorizado a sistemas informáticos com intenção criminosa** (Grabosky, 2016 *cit in* Maimon & Louderback, 2019). Associam-se ao *cyber-trespassing*, que implica a passagem não autorizada de barreiras invisíveis do ambiente virtual (Wall, 2001 *cit in* Maimon & Louderback, 2019).

O *hacking* inclui uma série de comportamentos, como o **redesenho de sistemas de *hardware* ou de *software***, para a modificação da sua função inicial, bem como a participação numa subcultura própria (Bachmann, 2010, Holt, 2007, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019). Implica uma atividade multi etápica, que poderá incluir: identificação e reconhecimento de sistemas de *hardware* ou *software* vulneráveis; infiltração nos alvos vulneráveis; alterações e redesenho dos sistemas alvo do ataque, incluindo a inserção de vírus e *malware* que permita acesso privilegiado a informação e dados (como, por exemplo, dados pessoais, *passwords*/credenciais de acesso e informação financeira/contas) ou mesmo o controlo do próprio sistema; ocultação da passagem e da modificação do sistema (Hughes & Delone, 2007, Wolfe et al., 2008, Holz et al., 2009, Waldrop, 2016, Luo & Liao, 2009 *cit in* Maimon & Louderback, 2019; Jahankhani et al., 2014).

Como a maioria dos crimes ciber-dependentes, também o *hacking* **medeia a prática de outros cibercrimes**, servindo como meio para que o cometimento de outros atos ilícitos seja possível e bem-sucedido, como o *hacking* de uma conta de *e-mail* em situações de *ciber-stalking* (Leukfeldt et al., 2006 *cit in* Leukfeldt et al., 2020) e o *DDoS* (ataque distribuído de negação de serviço).

No âmbito do *hacking*, são ainda propostas classificações diferenciadas de *hackers*, em função da sua intenção (Furnell, 2002 *cit in* Maimon & Louderback, 2019):

- ***White hat hackers*** (*hackers* cujo acesso não autorizado a sistemas tem como objetivo aumentar a segurança dos respetivos sistemas acedidos);
- ***Black hat hackers*** (*hackers* que acedem não autorizadamente a sistemas com intenção ilícita).

Há ainda uma diferenciação concetual que importará abordar: a classificação de *black hat hackers* aproxima-se do conceito de ***cracker***, enquanto alguém que, ao contrário do/a *white hat hacker*, se aproveita dos seus conhecimentos e do acesso não autorizado a sistemas informáticos para explorar a informação e dados que tem ao seu dispor, com fins ilícitos e/ou com o propósito de obter vantagem ou benefício pessoal.

1.3.2. *Spamming, Malware* e *DDoS* [ataque distribuído de negação de serviço]

O ***spamming*** ou ***SPAM***, acrómico da expressão "envio e publicação de publicidade em massa"[20], refere-se ao **envio de dados e à distribuição massiva** de *e-mails* que anunciam produtos, serviços ou esquemas de investimento, que podem ter um carácter fraudulento e inclusivamente conter *malware* ou outro anexo de arquivo executável (Rathi & Pareek, 2013).

O *spam* atende a três critérios:

- Anonimato – o endereço e a identidade do/a remetente estão ocultos ou omissos;
- Distribuição massiva – o *e-mail* é enviado para um grande grupo de pessoas/endereços eletrónicos;
- Não solicitado – o *e-mail* não é solicitado pelos/as destinatários/as (Rathi & Pareek, 2013).

O objetivo do *spam* é enganar ou convencer o/a destinatário/a relativamente ao anúncio de produtos, serviços ou esquemas atrativos. O/A remetente poderá solicitar dinheiro ou informações de segurança, como, por exemplo, o número do cartão de crédito ou outras informações pessoais, antes de o suposto acesso aos produtos ou serviços ocorrer (Jahankhani et al, 2014).

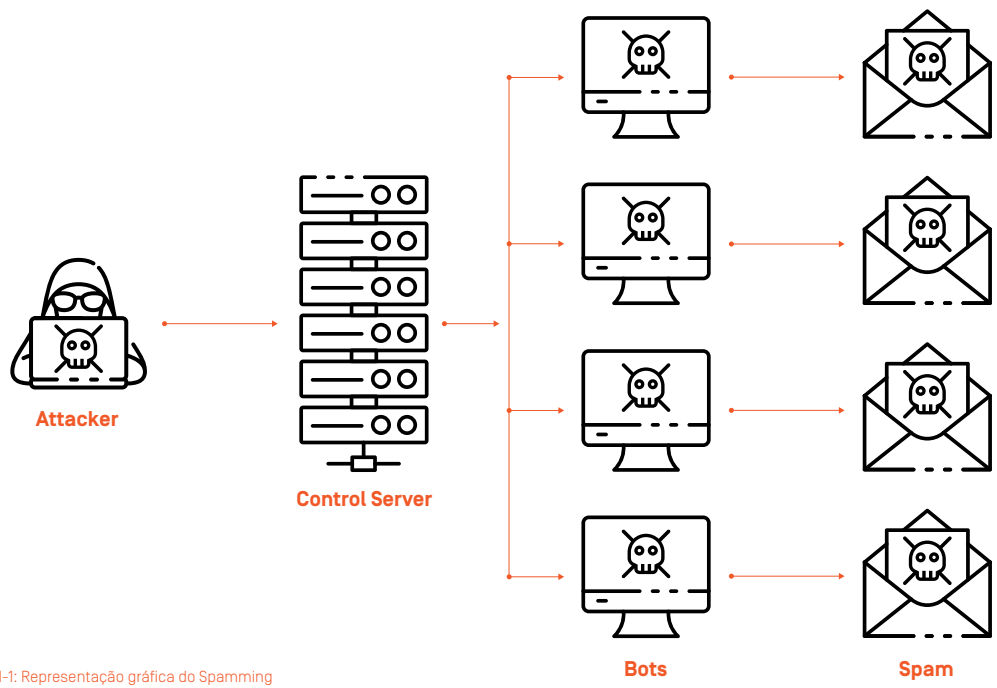

Figura I-1: Representação gráfica do Spamming

[20] Traduzido da expressão *Sending and Posting Advertisement in Mass.*

Já ***Malware*** é o termo utilizado para se referir a uma variedade de *softwares* de caráter hostil ou intrusivo (e.g., vírus de computador, *worms*[21], *ransomware*[22], *spyware*[23], *adware*[24], *scareware*[25], etc.).

Trata-se de ***software* destinado a infiltrar-se, de forma ilícita, em equipamentos**, com o intuito de causar danos, alterações ou furtar informação. O *malware* pode também assumir a forma de código executável, *scripts*, conteúdo ativo e outro *software* (Aycock, 2006 *cit in* Reep-van den Bergh & Junger, 2018).

Um dos esquemas frequentemente utilizados é a publicação de conteúdos com títulos que despertam curiosidade ou apelam a algum tipo de ação "urgente", bem como convites para instalar jogos ou sugestões para visitar perfis novos.

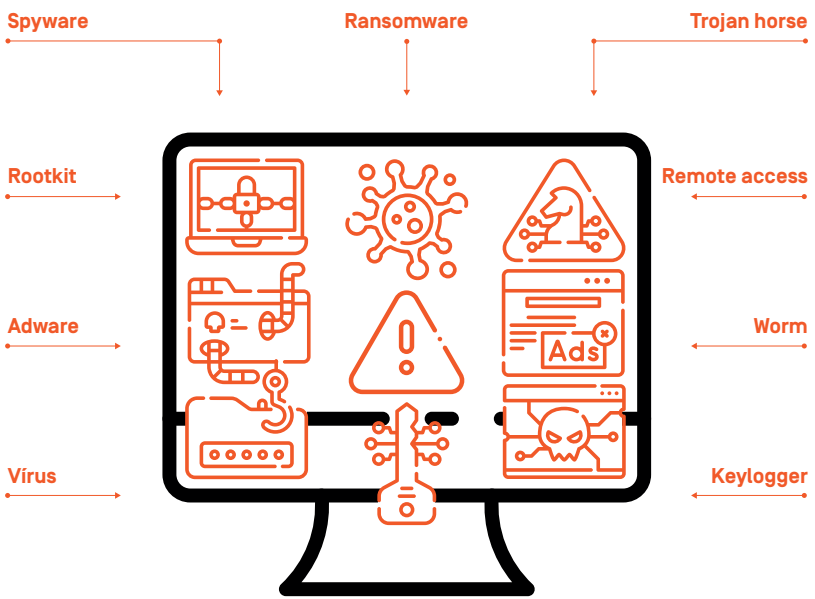

Figura I-2: Tipos de *Malware*

Por sua vez, o **ataque distribuído de negação de serviço (*DDoS*)**, diz respeito a uma tentativa intencional de sobrecarregar um determinado sistema informático (como o de estruturas governamentais ou grandes empresas, por exemplo), com o propósito de inviabilizar a sua utilização (Overvest & Straathof, 2015). A forma mais comum de perpetuar o ataque *DDoS* é através de *Botnet*. *Botnet* é uma rede de *bots* (computadores *zombie*) gerida pelo *botmaster* (*hacker*), através do servidor de comando e controle, que coordena e controla todos os dispositivos na rede. A instalação de uma *Botnet* depende de infeção anterior para obter o acesso ao sistema informático, normalmente por *malware*.

[21] *Worms* são códigos maliciosos que se propagam através de uma rede, com ou sem assistência humana (Kienzle & Elder, 2003).

[22] *Ransomware* é *malware* inserido no sistema por *download* e cria um arquivo "exe" para execução. O objetivo pode incluir a extorsão da vítima, criptografando as suas informações pessoais (Kansagra, Kumhar & Jha, 2016).

[23] *Spyware* é um programa automático que recolhe informações sobre o/a utilizador/a e sobre os seus hábitos de utilização da Internet e transmite essa informação a uma entidade externa, sem o conhecimento e consentimento do/a utilizador/a.

[24] *Adware* é designado como *software* que exibe ou descarrega automaticamente material publicitário (geralmente indesejado) quando o/a utilizador/a está *online* (Gao, Li, Kong, Bissyandé & Klein, 2019).

[25] *Scareware* é uma forma de *malware* que engana o/a utilizador/a, fazendo-o/a acreditar que o seu computador está infetado quando, na realidade, o sistema está a funcionar (Seifert, Stokes, Lu, Heckerman, Colcernian, Parthasarathy & Santhanam, 2015).

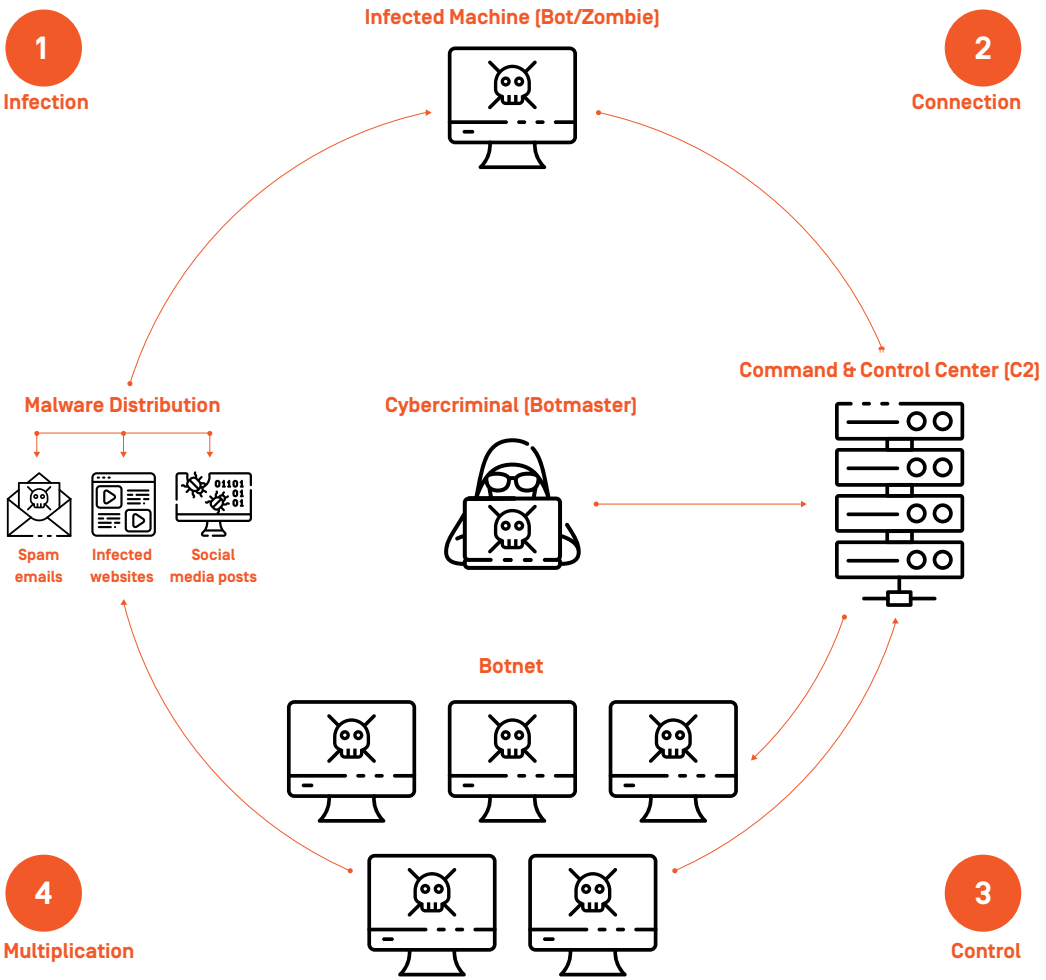

Figura I-3: Representação gráfica do funcionamento de uma *Botnet*

[37] PInformação adicional em https://www.stopbullying.gov/.

[38] Informação adicional e detalhada sobre o estudo está disponível em: 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.47f-deqj01ofo.

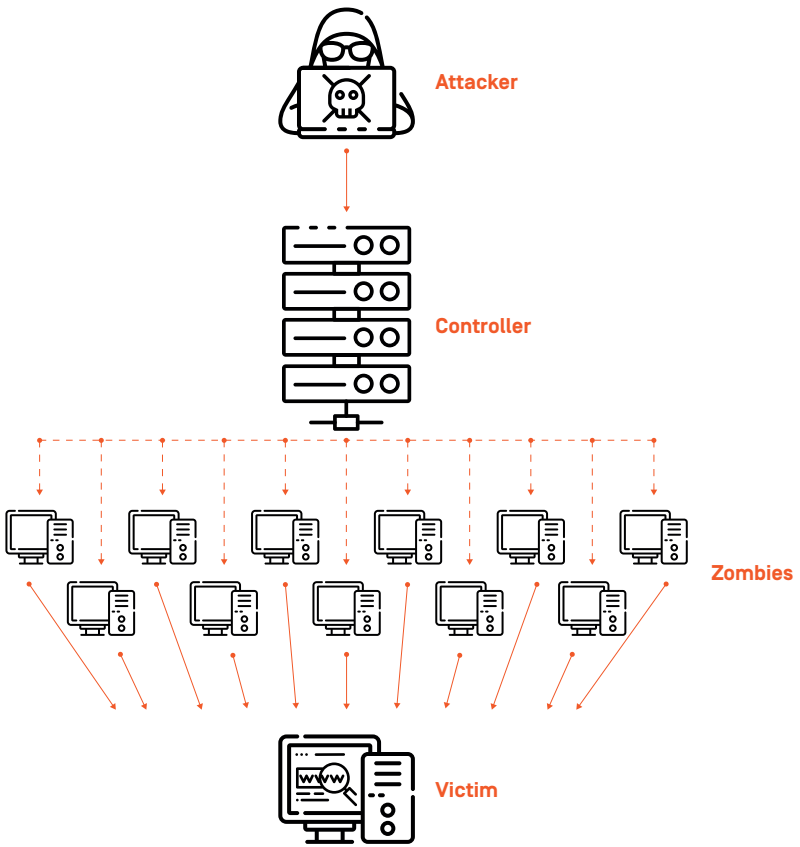

Figura I-4: Representação gráfica de um *DDoS*[26]

1.3.3. Burlas *online*

1.3.3.1. Burlas no comércio eletrónico[27]

As compras *online* são caracterizadas pela impossibilidade de analisar fisicamente os artigos, bens ou produtos, antes da realização da compra, e pela falta de contacto direto entre as partes envolvidas no processo de compra e venda (Moons, 2013, van Wilsem, 2013 *cit in* Reep-van den Bergh & Junger, 2018), aumentando o risco de burlas comércio eletrónico (ou *e-commerce*).

As burlas no comércio eletrónico apresentam **diferentes graus de complexidade**, desde esquemas

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

[27] Traduzido da expressão online shopping fraud.

simples, em que é prometido ao/à comprador/a o envio de determinado artigo, mediante transferência bancária prévia, acabando aquele por não receber o referido artigo (ou por rececionar um artigo distinto daquele que terá sido adquirido). Podem também as burlas assumir esquemas mais elaborados que, muitas vezes, envolvem a falsificação de documentos, como comprovativos de transferência bancária.

Ao nível das burlas e para a sua prática, também existe a possibilidade de exploração de vulnerabilidades em *websites* de compras *online* que armazenam dados bancários dos/as utilizadores/as (como dados de cartões de crédito ou débito), sendo estes ilicitamente acedidos e posteriormente utilizados por ciber-criminosos/as para venda na *dark web* ou para a realização de transações bancárias sem o conhecimento das vítimas (***card not present fraud***). O furto de dados bancários dos/as utilizadores/as para a prática deste tipo de burla ocorre normalmente através de *phishing*, fenómeno explorado em secções seguintes deste Manual.

1.3.3.2. Burlas em leilões na Internet[28]

A burla em leilões na Internet é um outro tipo de burla que ocorre quando os itens comprados são produtos falsos ou obtidos por meios ilícitos ou quando o/a vendedor/a anuncia ou disponibiliza para venda itens inexistentes. Neste tipo de fraude, é habitual o recurso a serviços de transferência bancária, facilitando-se a transação de dinheiro sem a necessidade de haver lugar à revelação da identidade dos/as intervenientes (Jahankhani et al., 2014).

A burla em leilões assenta no anonimato e também, por vezes, no recurso a dados falsos de identificação, aquando do registo nas plataformas ou *websites* nos quais os leilões decorrem.

Algumas das situações mais comuns envolvem:

- Aquisição/compra de itens que não chegam a ser rececionados pelos/as compradores/as;
- Itens pagos e rececionados que não correspondem aos itens desejados (e.g., o produto ou bem rececionado é significativamente distinto da descrição/registos fotográficos originais);
- Não divulgação ou divulgação incompleta de informações relevantes sobre o item e/ou as condições de venda;
- Não receção de pagamento por parte dos/as vendedores/as.

1.3.3.3. Burlas com cartão de crédito[29]

A burla com cartão de crédito refere-se à **utilização do cartão de crédito de outra pessoa para uso pessoal, sem o conhecimento do/a proprietário/a do cartão e da entidade emissora** (Patel & Singh, 2013). Existem vários métodos/crimes ciber-dependentes que poderão ser utilizados para a obtenção de acesso a tais cartões e a detalhes sobre o mesmo, como o *phishing*, o *spamming* ou o *hacking* (Jahankhani et al., 2014).

[28] Traduzido da expressão *internet auction fraud.*

[29] Traduzido da expressão *credit card fraud.*

Ainda no âmbito das burlas com cartão de crédito, destaque também para o ***skimming fraud***, que consiste na cópia da banda magnética de um cartão de pagamento, sem o conhecimento ou consentimento do/a titular do cartão, aquando da utilização do referido cartão num ATM (*automated teller machine* ou, em português, terminal de caixa automático) ou num terminal de ponto de venda. Após a cópia da banda magnética do cartão da vítima, os seus dados podem ser transmitidos eletronicamente para qualquer lado do mundo, possibilitando a realização de despesas/levantamentos presenciais nesses locais.

Recentemente têm vindo a verificar-se outro tipo de ataques, nomeadamente a máquinas ATM, num processo denominado de ***jackpotting***. O ataque a máquinas ATM pode ocorrer através da introdução de *malware* no sistema informático do equipamento/ATM ou através da ligação de *hardware*, denominado de "*Black-Box*", com o objetivo de levar as máquinas de multibanco a emitir o dinheiro que têm em caixa, através do comando do/a criminoso/a.

1.3.3.4. Burla nos relacionamentos íntimos[30]

As burlas nos relacionamentos íntimos ocorrem quando o/a agente procura estabelecer uma **relação de confiança e de intimidade**, nomeadamente através da Internet e das TIC, com um determinado alvo, como prelúdio para obter **benefício pessoal, nomeadamente financeiro e patrimonial**.

Nesta forma de burla, há habitualmente lugar à:

- Criação de perfil falso nas redes sociais, nas aplicações de encontros amorosos ou outras plataformas de *chat* e interação social;
- Estabelecimento de contacto com alvos aparentemente mais vulneráveis;
- Criação de vínculo emocional com o alvo previamente identificado;
- Desenvolvimento de uma narrativa com o intuito de extorquir património pessoal/financeiro ao alvo.

Este processo de sedução e de criação de uma relação com a vítima visa o acesso ao seu dinheiro ou outro património, contas bancárias, cartões de crédito, passaportes, contas de *e-mail* e/ou números de identificação pessoal. Pode também visar a coação da vítima para a prática de crimes em nome do/a autor/a.

1.3.4. Furto de identidade *online*

O furto de identidade abrange a **obtenção não consentida de dados pessoais e/ou confidenciais** de uma determinada vítima (como, por exemplo, nome, número de identificação pessoal, número do cartão de crédito, etc.), a sua **posse ou transferência** e **utilização** na prática de crimes.

[30] Traduzido da expressão online romance and dating scams.

Inclui, deste modo e de forma cumulativa, os seguintes atos:

- Obtenção de informações pessoais e/ou confidenciais sobre outra pessoa, sem o seu conhecimento;
- Posse ou transferência desses dados com a consciência de que serão utilizados para objetivos ilícitos;
- Utilização dos dados inicialmente obtidos para a prática de crimes.

Estes atos correspondem a **furto de identidade *online*** quando os dados pessoais e/ou confidenciais da vítima são obtidos através da Internet e/ou quando os dados obtidos, por qualquer meio, são transferidos através da Internet e/ou utilizados para a prática de um crime através da Internet.

Tem, por norma, como objetivos a obtenção de vantagem financeira, crédito e outros benefícios, a criação de desvantagem ou perda para a vítima (Enisa, 2010, Harrell & Lagton, 2013, Tuli & Juneja, 2015 *cit in* Reep-van den Bergh & Junger, 2018) e, inclusivamente, a prática de crimes em nome da vítima. A vítima cuja identidade foi utilizada, para além das perdas financeiras, poderá, deste modo, ser sujeita a consequências legais, caso seja responsabilizada pelas ações do/a autor/a.

O furto de identidade não é, em si mesmo, um crime, podendo englobar uma multiplicidade de crimes previstos e puníveis, ao abrigo do Código Penal português.

1.3.5. *Phishing*

O *phishing* traduz-se no envio em massa de mensagens de correio eletrónico - *spamming* -, habitualmente com uma hiperligação (*link)* para uma página da Internet, que os/as destinatários/as são persuadidos a aceder, apelando a motivos ou ações urgentes.

Por norma, estas mensagens de correio eletrónico solicitam ou apontam para a importância de os/as destinatários/as "atualizarem", "validarem" ou "confirmarem" informações bancárias.

Estas mensagens de correio eletrónico (e as páginas para as quais remetem) são falsas e constituem uma reprodução aproximada da comunicação original efetuada por entidades bancárias, entidades emissoras de crédito ou outras que permitam a realização de pagamentos *online*.

Aquando do acesso a tais páginas, é habitualmente solicitada a introdução de informação bancária do/a utilizador/a, sendo possível, a partir desse processo de inserção de dados bancários, a sua captura e posterior utilização indevida.

Deste modo, o *phishing* engloba diferentes atos ilícitos (Jahankhani et al., 2014) e diferentes etapas:

- Configuração de ***website*/página da Internet falsa**, que mimetiza um *website* fidedigno de

uma entidade idónea ou de confiança, normalmente uma entidade bancária. Este *website* ou página inclui um formulário de *login* ou registo e pode também redirecionar para o *website* ou página verdadeira da entidade bancária lesada, depois de utilizado o formulário.

- Criação de *e-mail* falso que, tal qual o *website*/página, mimetiza a comunicação efetuada por entidade idónea ou de confiança e **apela a uma atuação/ação urgente por parte do/a destinatário/a** (e.g., aviso de que os/as clientes necessitam de efetuar *login* imediatamente para impedir o bloqueio ou inativação das contas/dados de acesso), com posterior **envio massivo (*spamming*)**.
- **Obtenção de informações pessoais e/ou confidenciais** do/a destinatário/a, nomeadamente dados bancários, através do acesso por parte/a deste à hiperligação (*link*).
- **Utilização indevida**, por parte do/a autor/a do crime, dos dados bancários obtidos, para benefício económico e/ou para a prática de outros crimes.

DESTAQUE | ESTATÍSTICAS EM FOCO:

Segundo o Eurobarómetro 423[31], que visa analisar as perceções de cidadãos/ãs da União Europeia sobre utilização da Internet, cibersegurança e cibercriminalidade, 68% das pessoas inquiridas refere preocupação quanto ao **furto de identidade *online***, seguindo-se, por ordem decrescente, a preocupação com *software* malicioso/*malware* (66%), com **burlas *online***, nomeadamente burlas com cartões bancários (63%), e com o ***hacking*** das suas contas de *e-mail* e redes sociais (60%).

Adicionalmente, 47% dos/as inquiridos/as referiu já ter sido alvo de ***malware*** e 31% indicou ter já sido vítima de tentativas de ***phishing***.

1.3.6. Abuso e exploração sexual de crianças através da Internet

Por abuso sexual de crianças entende-se, segundo definição da Organização Mundial da Saúde – OMS (2017), o envolvimento da criança, ou seja, de qualquer pessoa com menos de 18 anos de idade, em atividade sexual:

- que a referida criança não compreende plenamente;
- relativamente à qual a criança não é capaz de consentir ou não está do ponto de vista do seu desenvolvimento preparada para consentir;
- que viola as leis em vigor.

Podem considerar-se tipos diferenciados de abuso sexual de crianças (OMS, 2017):

- **Abuso sexual sem contacto**, no qual se incluem as ameaças de abuso sexual, o assédio sexual, o aliciamento, a exposição da criança a conteúdos/materiais pornográficos, entre outras formas de abuso que não impliquem contacto direto entre vítima e agressor/a;

[31] Informação adicional e detalhada sobre este Eurobarómetro - Special Eurobarometer 423: *Cyber security* - está disponível em https://www.europeandataportal.eu/data/datasets/s2019_82_2_423_eng?locale=en.

- **Abuso sexual de contacto**, no qual se inserem, por exemplo, a prática de coito vaginal, anal e/ou oral com a criança, através de pénis, partes do corpo ou objetos, bem como outros atos sexuais, como beijar, acariciar e tocar.

A crescente e cada vez mais precoce **utilização da Internet e das redes sociais** por parte das crianças, aliada a uma reduzida, inexistente e/ou ineficiente supervisão familiar, aumenta a sua **exposição ao abuso e exploração sexual através da Internet** (Conselho da Europa, 2007 *cit in* APAV, 2019; Livingston & Smith, 2014).

DESTAQUE | ESTATÍSTICAS EM FOCO:

Segundo a base de dados *International Child Sexual Exploitation* (ICSE) - exploração sexual infantil - da INTERPOL[32], em 2018, verificaram-se mais de 1,5 milhões de imagens e vídeos e foram identificadas 19 400 crianças vítimas de abuso e exploração sexual em todo o mundo.

Após uma seleção aleatória de vídeos e imagens da referida base de dados ICSE, a INTERPOL e a ECPAT International publicaram, em 2018, um relatório conjunto intitulado *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*, com alguns resultados a destacar:

- 92% dos/as autores/as visíveis nos vídeos e imagens analisados são do sexo masculino;
- 65% das vítimas não identificadas são do sexo feminino;
- Mais de 60% das vítimas não identificadas incluíam bebés e crianças com menos idade;
- Quanto mais jovem é a vítima, mais grave é o abuso;
- 84% das imagens contêm material de abuso sexual de crianças, com atividade sexual explícita.

Em seguida, são abordadas algumas formas de abuso e exploração sexual de crianças através da Internet[33].

1.3.6.1. Abuso sexual de crianças *online*

O abuso sexual *online* pode ser definido enquanto conceito abrangente, contemplando **qualquer forma de abuso sexual de crianças em contexto *online***, no qual se incluem diferentes manifestações, desde o abuso sexual sem contacto, facilitado pelas TIC e pela Internet, redes sociais ou outras plataformas, como o assédio e o aliciamento, até à partilha de conteúdos na *dark web* (imagem e/ou áudio) de abuso e exploração sexual de crianças, previamente recolhidos em fotografia ou vídeo.

1.3.6.2. Exploração sexual de crianças *online*

O conceito de exploração sexual de crianças distingue-se de outras formas de abuso pelas noções de extração, de ganho e de benefício decorrentes da sujeição da criança a algum tipo de ato sexual.

[32] Informação adicional e detalhada está disponível em https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[33] Para informação detalhada relativamente a terminologia e diferentes formas de abuso e exploração sexual de crianças, queiram consultar *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse*, da EPCAT International e EPCAT Luxembourg, disponível em http://luxembourgguidelines.org/english-version/.

Sendo difícil a sua dissociação clara relativamente ao conceito de abuso sexual, por regra, a exploração sexual assenta no aproveitamento de uma característica, situação ou condição da criança, sendo os benefícios recolhidos pelo/a agressor/a, por terceiros ou até pela própria criança (como é o caso, por exemplo, da criança sujeita a situações de abuso sexual, em troca de afeto e carinho por pessoas adultas significativas).

Em sequência, na **exploração sexual de crianças *online*** incluem-se todos os atos de natureza sexual praticados contra uma criança que, em algum momento, apresentem algum tipo de ligação com as TIC, tais como:

- Exploração sexual realizada enquanto a criança vítima está a utilizar a Internet e as TIC, incluindo a sedução, a manipulação e a ameaça da criança para a prática atos sexuais perante *webcam*, por exemplo;
- Identificação e/ou preparação de potenciais vítimas *online*, com o objetivo de as explorar sexualmente (independentemente de a efetivação da exploração e abuso serem realizados *online* ou *offline*);
- Distribuição, divulgação, importação, exportação, oferta, venda, posse ou acesso consciente *online* a materiais de exploração sexual de crianças (mesmo que o conteúdo de abuso sexual contido no material tenha sido realizado *offline*).

1.3.6.3. Abuso sexual de crianças em direto

Este fenómeno envolve a **prática de atos sexuais com crianças e a sua transmissão em direto**, nomeadamente através de serviços de *live streaming*, sendo, deste modo, possível a sua visualização por outras pessoas. A visualização poderá implicar o pagamento prévio de determinado montante, podendo inclusivamente ser assignado aos/às espectadores/as a possibilidade de ditarem ou definirem o decurso dos atos de abuso e exploração sexual praticados contra a criança.

A transmissão em *live streaming* significa que os dados são transmitidos instantaneamente e com menor risco, uma vez que não requer o *download* de qualquer arquivo e, assim que a transmissão é interrompida, o material desaparece, dificultando, por isso mesmo, a investigação criminal, a recolha de provas e a identificação de vítimas e agressores/as.

O abuso sexual de crianças em direto envolve diferentes formas de abuso e exploração sexual de crianças, incluindo a produção e distribuição de materiais de abuso e de exploração sexual de crianças e a prostituição. Representa uma **forma dupla de vitimação** sexual da criança: primeiramente, esta é forçada ou, de algum modo, levada a participar em atividades sexuais, sozinha ou com outras pessoas; simultaneamente, a atividade sexual é transmitida em direto, através das TIC, e visualizada remotamente por outras pessoas.

1.3.6.4. Grooming online

O *grooming online* pode ser definido como um **processo de manipulação** e uma **forma de aliciamento** de crianças. Inicia-se geralmente através de uma abordagem não-sexual, nomeadamente através da Internet e das TIC, incluindo jogos *online* e redes sociais, de forma a estabelecer uma relação de confiança com a criança e a convencer a encontrar-se pessoalmente com outra pessoa, para que esta última possa consumar o abuso sexual. O estabelecimento de relação de confiança com a criança, mediado pela Internet e pelas TIC, pode ainda visar a persuasão da criança à produção e partilha de conteúdo sexual[34].

O *grooming online* permite aos/às autores/as a seleção do tipo de vítima que pretendem manipular e aliciar. Adicionalmente, o *grooming online* permite o aliciamento de um grande número de vítimas em simultâneo, entre outras vantagens para o/a autor/a do processo de manipulação e aliciamento *online*, como o anonimato, a preservação da sua real identidade e a gestão das demais "identidades" com as quais se apresenta junto dos alvos que seleciona.

Na sequência desta forma de abuso e exploração sexual, pode a criança ser sujeita a ameaças e chantagem de divulgação ou partilha dos conteúdos sexuais auto produzidos, tendo o/a aliciador/em vista a obtenção de favores sexuais, dinheiro ou outros benefícios. Este fenómeno designa-se por **extorsão sexual de crianças**.

DESTAQUE | PRÁTICAS EM FOCO:

A *Childline*[35] é um serviço gratuito e confidencial disponibilizado especificamente a crianças e jovens, no Reino Unido, dedicando-se a uma ampla gama de temáticas e problemas que podem afetar estes grupos etários.

Entre diversos temas, o serviço dispõe de informação sobre comportamentos de segurança na utilização da Internet e das TIC, bem como um mecanismo *online* para denúncia de partilha/divulgação de conteúdos sexuais auto produzidos.

O mecanismo de denúncia está disponível em: https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/sexting/report-nude-image-online/.

1.3.6.5. Material de abuso sexual e de exploração sexual de crianças *online*[36]

DESTAQUE | ESTATÍSTICAS EM FOCO:

De acordo com o já citado Eurobarómetro 423, 7% das pessoas inquiridas referiu já ter sido acidentalmente exposta a **material de abuso e de exploração de crianças *online***.

[34] No âmbito do conteúdo sexual auto produzido, poderemos incluir, a título de exemplo, o *sexting*, enquanto forma de autoprodução de conteúdos – texto, imagens e/ou vídeos - de natureza sexual e sua partilha, habitualmente de forma consentida e entre pares. Pode, todavia, a sua produção ser realizada sob pressão ou coação ou mesmo levar à partilha não consentida do conteúdo produzido.

[35] Informação adicional e detalhada esta disponível em: https://www.childline.org.uk/.

[36] Traduzido das expressões *child sexual abuse material* e *child sexual exploitation material*.

As expressões **material de abuso sexual de crianças e material de exploração sexual de crianças** procuram substituir, pelo menos em contextos não legais ou jurídicos, o conceito de pornografia infantil (terminologia ainda constante em legislação nacional e internacional), dizendo, respetivamente, respeito:

- 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.

Esta mudança de terminologia baseia-se no argumento de que qualquer material que represente uma criança de forma sexualizada é, de facto, uma forma de abuso e de exploração sexual de crianças e não deverá ser descrito enquanto "pornografia".

O **material de abuso e de exploração sexual de crianças gerado digitalmente ou através de computador**, seja de forma total ou parcial, é também considerado material de abuso e de exploração sexual de crianças.

1.3.7. *Ciber-bullying, ciber-stalking* e outras formas de agressão *online* nas relações interpessoais

O *bullying* é um fenómeno de violência entre pares que implica ou envolve a perpetração de comportamentos agressivos e violentos por um/a agressor/a ou grupo de agressores/as contra uma vítima ou grupo de vítimas, com o objetivo de a(s) prejudicar, de lhe(s) causar dano ou sofrimento (APAV, 2011).

Por sua vez, o ***ciber-bullying*** emerge da utilização das TIC e da Internet, com o objetivo de agredir verbalmente a vítima e/ou contribuir para a sua exclusão e isolamento social. Alguns dos comportamentos que operacionalizam esta forma de agressão *online* poderão incluir: a disseminação de informação negativa/falsa com intenção de difamar a vítima (pelo recurso a telefonemas, mensagens de texto, mensagens de vídeo, *e-mail*, *chat room*, *websites*, redes sociais); importunação da vítima (pelo recurso aos mesmos meios) (APAV, 2011; Jahankhani et al., 2014).

O *ciber-bullying* distingue-se das modalidades mais convencionais de *bullying* pela possibilidade de ser praticado em qualquer altura do dia, independentemente da necessidade de contacto direto entre vítima e agressor/a, pelo potencial de anonimato que garante ao/à agressor/a, pelo elevado potencial de "publicidade" e audiência a que está associado (podendo ser infinitamente partilhado nas redes sociais ou qualquer outra plataforma de comunicação através da Internet em que foi iniciado/publicado e mesmo entre plataformas) e pela dificuldade de remoção do conteúdo criado[37].

[37] Informação adicional em https://www.stopbullying.gov/.

1. CIBERCRIME: UMA ABORDAGEM À SUA CONCETUALIZAÇÃO

DESTAQUE | ESTATÍSTICAS EM FOCO:

Segundo os resultados do inquérito realizado pela EU KIDS *ONLINE*[38], envolvendo 19 países da União Europeia sobre a utilização da Internet e as práticas e experiências online de crianças entre os 9 e os 16 anos de idade, em média, 5% das crianças referiu ter sido vítima de ***ciber-bullying***, ao longo dos últimos 12 meses anteriores ao estudo.

Ainda no mesmo inquérito, cerca de 22% das crianças participantes referiu já ter recebido **mensagens com conteúdo sexual**. Veja-se campos anteriores, nos quais são abordadas diferentes formas de abuso e exploração sexual de crianças através da Internet.

Já de acordo com os dados mais recentes do estudo transnacional *Health Behaviour in School-aged Children*[39], regularmente realizado pela Organização Mundial da Saúde (OMS), a prevalência da vitimação por ***ciber-bullying*** revela-se superior à identificada no inquérito anterior: respetivamente, 12% e 14% dos adolescentes do sexo masculino e do sexo feminino relataram ter sido vítimas de *ciber-bullying*.

No que às diferentes formas de expressão do *ciber-bullying* diz respeito, poderemos destacar as condutas de agressão *online* com cariz sexual, como:

- A partilha *online* de boatos ou mentiras sobre o comportamento sexual da vítima;
- O uso de linguagem sexual ofensiva ou discriminatória *online* dirigida contra a vítima;
- O furto de identidade para a partilha de conteúdo sexual e/ou para o assédio sexual contra outra pessoas, em nome da vítima;
- A partilha de informação *online* referente à intimidade da vítima, de forma não consensual, como estratégia para perpetuar os comportamentos de agressão e assédio em larga escala.

Poderemos igualmente salientar o *body shamming* através da Internet e das TIC, enquanto partilha de comentários depreciativos relativos ao aspeto físico da vítima, e o *outing*, quando alguém revela (ou ameaça revelar) publicamente, através da Internet e das TIC, informação relativa à orientação sexual ou identidade de género da vítima, sem o seu conhecimento e autorização.

Já o ***ciber-stalking*** pode ser definido como uma forma de *stalking* que, mantendo o carácter intrusivo, repetitivo e persistente que causa medo à vítima e que caracteriza esta forma de perseguição e assédio persistente, é praticado com recurso à Internet e às TIC, com o objetivo de ameaçar e assediar a vítima (Maran & Begotti, 2019).

As práticas de *ciber-stalking* poderão incluir, entre diferentes comportamentos de perseguição: efetuar várias e indesejadas tentativas de contacto com a vítima, via telefone, *e-mail* e redes sociais; instalar *spyware* no computador da vítima; aceder, sem autorização da vítima, ao seu *e-mail* e/ou conta das redes sociais, para monitorizar informação privada e o quotidiano da vida da vítima e/ou para agir em seu nome (Martellozzo & Jane, 2017).

[38] Informação adicional e detalhada sobre o estudo está disponível em: 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.47f-deqj01ofo.

[39] Informação adicional e detalhada está disponível no relatório do estudo: 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.

O *ciber-stalking* pode anteceder a prática de outras formas de *stalking* em contextos convencionais ou mesmo decorrer no âmbito de uma campanha de perseguição e assédio que decorre tanto *online*, como *offline*. Os/As agressores/as podem ser pessoas que a vítima conhece, incluindo amigos/as e colegas de trabalho, bem como ex-companheiros/as ou pessoas desconhecidas (Maran & Begotti, 2019).

DESTAQUE | ESTATÍSTICAS EM FOCO:

Segundo um inquérito europeu sobre violência contra as mulheres[40], das mais de 40 000 mulheres inquiridas nos diferentes Estados-Membros da União Europeia, 5% referiu ter sido vítima de alguma forma de ***ciber-stalking***, desde os 15 anos de idade.

De entre os Estados-Membros, destacou-se a Suécia (com uma prevalência de 14%) e, no campo oposto, a Espanha (com 2% de prevalência).

Ainda no âmbito da violência *online* no contexto de relações interpessoais, poderemos destacar, para além do *ciber-bullying* e do *ciber-stalking*, a **divulgação não consensual de imagens e vídeos**, enquanto partilha de imagens íntimas, incluindo fotografias, filmes e/ou gravações de vídeo, sem o consentimento da pessoa que vê a sua nudez, partes do corpo, incluindo órgãos sexuais, e/ou atividade sexual expostas.

As motivações para a divulgação deste conteúdo podem ser:

- A **extorsão ou coação sexual da vítima**, na qual o/a autor/a do crime, depois de receber, normalmente de forma consensual, vídeos e/ou fotografias de cariz sexual da vítima, ameaça a sua divulgação, caso a vítima não forneça novos conteúdos auto produzidos de natureza sexual ou não aceda a um encontro pessoal com o/a agressor/a.

- A **vingança**, frequentemente designada por *revenge porn*, que implica a divulgação não consensual de imagens íntimas - fotografias, filmes e/ou gravações de vídeo – de um/a companheiro/a, habitualmente após o término do relacionamento, enquanto forma de retaliação. Trata-se de um fenómeno comum no âmbito da violência nos relacionamentos íntimos, nos quais, na sequência da rutura relacional, são divulgadas imagens e/ou vídeos sexuais (ou é ameaçada a sua divulgação) do/a ex-companheiro/a, junto de familiares e amigos/as, através das redes sociais ou mesmo em websites pornográficos.

[40] Informação adicional e detalhada sobre os resultados do inquérito europeu da *European Union Agency for Fundamental Rights* está disponível em https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf.

DESTAQUE | PRÁTICAS EM FOCO:

O Facebook® disponibiliza, em *Not Without My Consent*, um leque de recursos de informação associados à extorsão sexual e à divulgação não consensual de imagens e vídeos.

Not Without My Consent dispõe ainda de um espaço para denúncia de situações de partilha/divulgação não consensual de imagens e vídeos, bem como de um guia com instruções para a remoção de conteúdo *online*.

Informação adicional e detalhada está disponível em: https://www.facebook.com/safety/notwithoutmyconsent.

1.3.8. Outras formas de cibercrime

O **ciberterrorismo** é uma forma de terrorismo que usa informações, computadores, redes e infraestrutura técnica para conduzir atividades terroristas. Devido à importância desses componentes de interconexão de redes, o ciberterrorismo poderá ser considerado potencialmente mais prejudicial do que o terrorismo *tradicional*. Em particular, o ciberterrorismo tem como alvo a infraestrutura financeira e comercial, bem como a infraestrutura governamental, o controlo de tráfego aéreo e registos médicos, apresentando como vantagens o facto de poder ser realizado com recursos financeiros modestos, com anonimato e à distância (Hansen, Lowry, Meservy & McDonald, 2007).

A intenção do ciberterrorismo é **incapacitar e/ou reduzir drasticamente a disponibilidade dos recursos computacionais de uma organização, entidade ou infraestrutura**: para uma empresa privada, este tipo de ataque poderá resultar em perdas financeiras; para uma entidade governamental, poderá convergir na incapacidade de cumprir a sua missão (Kratchman, Smith & Smith, 2008).

O conceito de ciberterrorismo associa-se, aliás, ao de destruição e/ou incapacitação de **infraestruturas críticas**, cujo comprometimento tem um impacto debilitante na segurança nacional, na economia e no estado social de um determinado país (Dunn & Wigert, 2004 *cit in* Yar & Steinmetz, 2019). No âmbito destas infraestruturas críticas, poderemos incluir as comunicações, a energia, a água, a comida, os serviços de emergência e os serviços de saúde, assim como símbolos de coesão nacional (Milone, 2003 *cit in* idem). De entre estas infraestruturas, destacam-se as dos setores da informação e telecomunicações, pelo seu papel central no funcionamento das demais infraestruturas críticas de um país (Dunn & Wigert, 2004 *cit in idem*).

Para a sua prática, poderão ser cometidos diversos dos crimes ciber-dependentes já referidos ao longo deste Manual.

Numa outra nota, poderemos incluir os **discursos de ódio *online***, nos quais se incluem todas as formas de comunicação e expressão, nomeadamente através da Internet e das TIC, que promovem,

disseminam, incitam ou justificam o ódio racial, a xenofobia, o antissemitismo e outras formas de ódio baseado na intolerância contra uma pessoa ou grupo de pessoas.

DESTAQUE | ESTATÍSTICAS EM FOCO:

No *Flash Eurobarometer 469 – June 2018*[41], os/as inquiridos/as foram questionados sobre o tipo de conteúdo ilegal acidentalmente descoberto *online*. De entre várias opções, o **discurso de ódio** foi o tipo de conteúdo ilegal mais mencionado em 10 países, particularmente em Malta (55%), na República Checa (53%), na Bulgária (52%) e na Polónia (50%).

As pessoas inquiridas que referiram ter visualizado pelo menos um tipo de conteúdo ilegal *online*, foram questionadas sobre a sua atuação:

- 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%).

A crescente utilização da Internet, das TIC e das redes sociais foi acompanhada pela proliferação do **discurso de ódio** *online* **contra determinados grupos de pessoas** (Banks, 2010 cit in Martellozzo & Jane, 2017). Tal proliferação assenta num conjunto de características associadas à Internet e às TIC, das quais poderemos destacar (Yar & Steinmetz, 2019):

- Constitui uma ferramenta de baixo custo e eficiente, assente num reduzido investimento financeiro, com capacidade de disseminar o discurso de ódio junto de audiências alargadas;
- Apresenta menor risco de deteção e identificação, pelo anonimato e preservação da identidade que proporciona na sua utilização para estes fins;
- Permite acesso a canais de comunicação que, de outro modo, não estariam disponíveis para a disseminação deste tipo de discursos;
- Permite a adaptação do conteúdo e do formato de transmissão de informação em função da audiência e dos grupos-alvo.

DESTAQUE | PRÁTICAS EM FOCO:

Em maio de 2016, a Comissão Europeia e quatro plataformas digitais (Facebook®, Youtube®, Twitter® e Microsoft®) anunciaram um **Código de Conduta contra o Discurso de Ódio *Online***[42], ao qual outras empresas aderiram.

Um dos objetivos deste código é a remoção mais imediata possível dos conteúdos de discurso de ódio *online*, nomeadamente em 24 horas, com o propósito de atingir o menor público possível.

[41] Informação adicional e detalhada está disponível em https://ec.europa.eu/digital-single-market/en/news/flash-eurobarometer-illegal-content.

[42] O Código de Conduta e informação adicional sobre a sua criação e implementação estão disponíveis em https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1135.

1.4. As cifras negras associadas ao cibercrime

Os números de cibercriminalidade que temos vindo a sintetizar ao longo dos pontos anteriores deste Manual não retratam, apesar da sua expressividade e dimensão significativa, a realidade efetiva da cibercriminalidade.

A prevalência exata da cibercriminalidade é desconhecida. Poderá tratar-se, provavelmente, de uma **elevada dimensão de cibercrimes indetetáveis, não reportados, não investigados e não resolvidos**, atendendo à invisibilidade e à complexidade da prova digital associada à sua ocorrência, a eventuais lacunas na legislação necessária e mesmo à natureza frequentemente transnacional da cibercriminalidade (Koops, 2010; Cangemi, 2004 *cit in* Yucedal, 2010).

Identicamente, a relutância generalizada das vítimas de cibercrime relativamente à denúncia (Koops, 2010), seja por receio, por desconhecimento e/ou por desvalorização dos atos de que foram alvo, também contribui significativamente para o desconhecimento da real dimensão da cibercriminalidade.

São várias as explicações que fundamentam a não denúncia de situações de cibercrime e, consequentemente, o desfasamento entre a dimensão de cibercrimes que chega ao conhecimento das autoridades competentes e a cibercriminalidade "real" (Goucher, 2010; Kanayamaa, 2017; Maimon & Louderback, 2019; Leukfeldt et al., 2020), de entre as quais destacamos:

- O desconhecimento ou não reconhecimento das vítimas de cibercrime dos atos de que foram alvo enquanto formas de criminalidade;
- Sentimentos de vergonha, culpa e auto responsabilização pela cibervitimação de que foram alvo;
- A desvalorização dos danos e perdas causadas pelo cibercrime;
- A relutância ou resistência das vítimas relativamente à denúncia do cibercrime junto das autoridades competentes;
- A não identificação de benefícios associados à denúncia do cibercrime junto das autoridades competentes, atendendo ao insucesso a que, muitas vezes, estão condenadas as investigações de cibercrime e ao aparente reduzido dano causado pelo cibercrime (pelo menos, no que respeita ao dano e impactos sentidos/percecionados por cada vítima, a título individual);
- A falta de familiarização e de conhecimento de alguns agentes das forças de segurança relativamente ao cibercrime;
- A escassez de formação específica transversal a todas as forças de segurança relativamente ao cibercrime e a falta de recursos financeiros para a prossecução da investigação;
- A ausência de respostas ou serviços de apoio específicos ou especializados, diferenciados das respostas tradicionais dirigidas a vítimas de crimes "convencionais", que possam auxiliar a vítima de cibercrime na obtenção de ajuda/na articulação com os recursos disponíveis;
- A inexistência de sistemas e mecanismos acessíveis (nomeadamente através da Internet) e simples de denúncia de situações de cibercriminalidade.

1. CIBERCRIME: UMA ABORDAGEM À SUA CONCETUALIZAÇÃO

Pese embora a relevância das fundamentações anteriores, destacamos, ao longo deste Manual, a título exemplificativo e não exaustivo, algumas respostas, serviços e mecanismos existentes, que dão conta dos esforços realizados para a promoção e facilitação do acesso a serviços de apoio, a informação, bem como a mecanismos *online* para a denúncia de situações de cibercrime.

DESTAQUE | PRÁTICAS EM FOCO:

A EUROPOL - *European Union Agency for Law Enforcement Cooperation* disponibiliza, no seu *website*, um espaço onde é possível aceder aos mecanismos de denúncia de cibercrime (inclusivamente de denúncia *online*, quando aplicável) existentes em diferentes Estados-Membros.

Esse espaço está disponível em: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online.

DESTAQUE | PRÁTICAS EM FOCO:

Action fraud é o um centro nacional de denúncias do Reino Unido para casos de burlas *online* e outros cibercrimes.

Para além de apoio telefónico disponibilizado, o *Action fraud* disponibiliza uma ferramenta de denúncia *online*, acessível em: https://reporting.actionfraud.police.uk/login.

No caso do **abuso e exploração sexual de crianças através da Internet**, outros obstáculos se associam à revelação da experiência de vitimação por parte da criança vítima, como:

- Sentimentos de culpa e de vergonha pelas situações de cibervitimação de que possa ter sido vítima;
- Sentimento de (auto)responsabilização, por se percecionar, de algum modo, cúmplice ou conivente com a situação de cibervitimação;
- Medo de represálias por parte do/a autor/a do cibercrime e/ou de castigos por parte dos responsáveis legais, em caso de revelação;
- Receio de ser desacreditada;
- Medo de perder recompensas que possa receber do/a autor/a dos atos de abuso e exploração sexual, como contrapartida da prática, da participação e/ou da produção de conteúdos de natureza sexual;
- Não identificação das situações de abuso e de exploração sexual como atos ilícitos e/ou interpretação dos mesmos como manifestações de afeto.

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

DESTAQUE | PRÁTICAS EM FOCO:

A INHOPE[43] que é uma rede atualmente composta por 46 linhas de denúncia (*hotlines*) de diversos países, incluindo os Estados-Membros da União Europeia, destinadas ao combate ao material de abuso e exploração sexual de crianças *online*.

A Associação Portuguesa de Apoio à Vítima (APAV) é responsável, em **Portugal**, pela operação da Linha Internet Segura, ao abrigo do consórcio Centro Internet Segura, promovido pela Fundação para a Ciência e a Tecnologia. No que à intervenção da Linha Internet Segura diz respeito, para além para prestação de apoio e informação sobre questões de segurança na Internet, está disponível uma plataforma que permite e facilita a **denúncia anónima de conteúdos ilegais na Internet**, com destaque para o material de abuso e de exploração sexual de crianças *online* e para o incitamento e promoção do racismo, xenofobia e outras formas de violência.

A plataforma de denúncia está disponível em: https://www.internetsegura.pt/.

Na **Alemanha**, o *Safer Internet Center*[44] é também uma plataforma que disponibiliza informação de segurança sobre a utilização da Internet dirigida à família, a crianças e jovens e a professores. Inclui igualmente linhas telefónicas de apoio e uma plataforma de denúncia de material de abuso e exploração sexual de crianças *online*: https://www.jugendschutz.net/hotline/.

Igualmente, na **Roménia**, um dos países que integra também a INHOPE, através da Save the Children Romania, está disponível um mecanismo/formulário eletrónico que facilita a denúncia de conteúdos ilícitos *online*. Veja-se, para o efeito, https://oradenet.salvaticopiii.ro/esc-abuz.

Já no que diz respeito à **cibercriminalidade contra entidades coletivas**, nomeadamente organizações e empresas, sejam elas de pequena ou de grande dimensão, os estudos apontam para prevalências elevadas de cibercrime, nomeadamente de **crimes ciber-dependentes** (Rantala, 2008 *cit in* Maimon & Louderback, 2019; Saini, Rao & Panda, 2012). Paradoxalmente, as taxas de denúncia identificadas são francamente diminutas, o que poderá associar-se, entre outros motivos:

- Ao receio do comprometimento da reputação da entidade, da sua imagem pública e/ou da marca, produtos e/ou serviços que providencia;
- Ao receio de perda de confiança da sociedade e de cidadãos/ãs na intervenção da entidade e na qualidade e fiabilidade da mesma;
- À minimização de eventuais perdas financeiras associadas a potenciais impactos nas dimensões anteriormente indicadas;
- Ao facto de os cibercrimes terem sido praticados por alguém interno à própria entidade.

[43] Informação adicional e detalhada está disponível em https://www.inhope.org/EN.

[44] Informação adicional e detalhada está disponível em https://www.saferinternet.de/.

2. O ENQUADRAMENTO JURÍDICO DO CIBERCRIME

2.1. Cibercrime à luz do Conselho da Europa

Tendo em conta a necessidade de salvaguardar direitos fundamentais no espaço cibernético, vulgo ciberespaço, bem como as pesadas consequências socioeconómicas associadas à prática de cibercrimes, a regulação penal de condutas ilícitas que têm na sua essência ou como elemento facilitador o recurso a meios informáticos é crucial. Neste sentido, a condenação expressa destas condutas e sua constante atualização carrega em si não só uma mensagem de dissuasão para eventuais agentes do crime, mas também de que o combate ao cibercrime está cada vez mais no topo das agendas políticas dos Estados.[45]

O instrumento internacional de maior relevo na área do cibercrime é a Convenção sobre o Cibercrime do Conselho da Europa, de 23 de Novembro de 2001, destinada a «proteger a sociedade do cibercrime, *inter alia*, através da adoção de legislação adequada e da melhoria da cooperação internacional», de modo a «tornar mais eficazes as investigações e os processos penais respeitantes às infrações penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de prova, em formato eletrónico».[46] Com este fim, a Convenção impõe aos Estados signatários que adequem o seu Direito Penal substantivo e adjetivo interno às especificidades destes crimes, tendo como objetivo a harmonização de legislações, incluindo instrumentos processuais e de produção de prova adequados e simplificação da cooperação internacional, de modo a facilitar e agilizar a deteção, investigação, recolha de prova e perseguição. Por fim, busca também a harmonização do direito penal material e, de modo a potenciar a perseguição e investigação pelas autoridades policiais e judiciais, a Convenção sugere ainda a implementação de medidas específicas processuais adequadas a este tipo de criminalidade e promove a cooperação internacional.

No que concerne à proteção contra abuso e exploração sexual de menores, o documento timoneiro é a Convenção sobre Proteção de Crianças contra Exploração e Abuso Sexual, vulgarmente conhecida como a Convenção de Lanzarote.[47] Em vigor desde 1 de Julho de 2010, alargou os ilícitos criminais de modo a abranger todos os tipos possíveis de crimes sexuais contra crianças. De particular relevo em sede de cibercrime é a tipificação das condutas de aliciamento de crianças através da exposição a conteúdos sexuais e ilícitos relacionados com conteúdos de exploração e abuso sexual de menores. A Convenção abrange ainda o abuso sexual no âmbito da família da criança ou "círculo de confiança", bem como atos realizados com fins comerciais ou lucrativos. Desta feita, os Estados são instados a desenvolver legislação específica que criminalize todas as condutas referidas na Convenção, a investigar e indiciar os agentes do crime, a promover medidas de prevenção tendo em conta o superior interesse da criança. Por fim, é também promovida a cooperação internacional entre estados.[48]

2.2. Cibercrime no Direito da União Europeia

No âmbito da União Europeia (EU), vários instrumentos têm vindo a ser adotados na área do cibercrime. Em 2013, através de uma comunicação conjunta ao Parlamento Europeu, ao Conselho, ao Comi-

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

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

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

[48] Para mais informações, consultar https://rm.coe.int/information-note-the-council-of-europe-convention-on-the-protection-of/16807962a7.

té Económico e Social Europeu e ao Comité das Regiões foi definida a Estratégia da União Europeia para a Cibersegurança[49] definindo como pilares fundamentais para essa estratégia a harmonização de políticas e criação de mecanismos de cooperação entre Estados-Membros, de modo a assegurar cibersegurança e o respeito pelos princípios democráticos da EU. Para esse efeito, propõe a criação de legislação adequada em matéria de cibersegurança, visando o desenvolvimento dos meios industriais e tecnológicos para garantir a segurança digital e a criação de unidades nacionais de combate ao cibercrime. Nesse sentido, a comunicação prevê sinergias com o setor privado com vista à criação de resiliência digital. Por outro lado, prevê também medidas de prevenção como campanhas de sensibilização e formação especializada sobre o fenómeno. A comunicação apela ainda ao investimento em pesquisa científica e tecnológica de modo a colmatar as lacunas tecnológicas existentes nos Estados Membros. Por fim, a comunicação dispõe sobre como reagir a eventuais ataques cibernéticos de espionagem de países terceiros. As áreas de combate prioritário deverão ser o abuso sexual de menores, pagamentos fraudulentos, *botnets* e interferências não autorizadas em sistemas informáticos.

Face ao aumento exponencial de crimes informáticos nos últimos anos, o Parlamento Europeu adotou uma resolução sobre a luta contra o crime informático, no dia 3 de outubro de 2017[50]. No seu texto a resolução refere que os membros do Parlamento Europeu "condenam qualquer ataque informático realizado ou dirigido por uma nação estrangeira ou seus agentes para interromper o processo democrático de outro país." Além disso, o Parlamento Europeu salienta que a "consciencialização sobre os riscos apresentados pelo crime informático aumentou, mas as medidas preventivas tomadas por utilizadores individuais, instituições públicas e empresas permanecem totalmente inadequadas, principalmente devido à falta de conhecimentos e recursos."

A resolução identifica os eixos principais no combate ao cibercrime destacando a prevenção, assegurar que as vitimas beneficiem plenamente dos direitos consagrados na Diretiva 2012/29/EU, proteção dos direitos das crianças, reforço da responsabilidade dos provedores de serviço de internet a fim de obter maior qualidade dos produtos e mais segurança, melhoria dos mecanismos de cooperação entre as autoridades policiais, judiciais e provedores de serviço de internet, adoção de uma política comum em matéria de justiça penal no ciberespaço que será, por sua vez, crucial na obtenção e preservação da prova eletrónica, reforço das capacidades informáticas e tecnológicas, aumento da cooperação com países terceiros.

A EU encontra-se, deste modo, num processo de modernização constante das suas diretivas, de modo a garantir que a mesmas se mantenham atualizadas de modo a combater eficazmente novas ameaças. Elencam-se, assim, os principais instrumentos vinculativos a nível da EU relativos à cibercriminalidade:

A propósito da cibercriminalidade *strictu sensu*;

Diretiva 2011/93/UE – **Relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho**[51], criada para

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

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

[51] Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de Dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32011L0093&from=PT.

fazer face aos novos fenómenos criminais associados ao abuso e exploração sexual de menores, aliciamento e pornografia infantil *online*. Para esse efeito, a Diretiva define crimes, sanções e circunstâncias agravantes, bem como penas privativas de liberdade mínimas, a punibilidade da tentativa e de diferentes formas de autoria, como é o exemplo da cumplicidade, e a responsabilidade criminal de pessoas coletivas, assim como obrigatoriedade de existirem bases de dados de infratores, de modo a prevenir a reincidência. Por fim, a Diretiva urge à cooperação entre entidades públicas e privadas na proteção, assistência e apoio às vítimas e à obrigatoriedade de formação especializada para todos os intervenientes no processo penal. A este respeito, a Diretiva estabelece também garantias processuais especiais para as vítimas, para além das já definidas na Diretiva que estabeleceu o Estatuto da Vítima[52]. Por fim, estabelece a existência de programas de intervenção preventiva, de prevenção e de medidas de intervenção durante ou após o processo penal. Esta legislação foi transposta para os ordenamentos nacionais dos Estados Membros em 2013. Já foram elaborados dois relatórios sobre a implementação da diretiva pelos Estados Membros em 2016.

Diretiva 2013/40/UE – **Relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho**[53], tem como propósito regulamentar ataques informáticos de larga escala de modo a que os Estados Membros reforcem as suas legislações nacionais nesta matéria e definam infrações penais e sanções para os infratores, bem como a responsabilidade criminal de pessoas coletivas. A Diretiva também visa melhorar a cooperação entre autoridades competentes e Estados-Membros. Esta diretiva foi transposta para os ordenamentos jurídicos internacionais dos Estados-Membros em 2015.

Diretiva (UE) 2019/713 – **Relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho**[54], esta diretiva pretende complementar a diretiva 2013/40/EU, no sentido de abranger como ilícitos criminais as condutas na esfera digital tendentes ao furto, roubo, ou qualquer outra forma de apropriação ilícita, contrafação ou falsificação, posse ou aquisição de novos meios de pagamento tecnológicos, que não em numerário, bem como respetivas sanções mínimas. Esta nova diretiva consagra, portanto, não só infrações relacionadas com meios de pagamento corpóreos que não em numerário (por exemplo, MBway), mas também não corpóreos, como todas transações realizadas eletronicamente (por exemplo, transações feitas em moeda virtual). Assim, a definição de meios de troca digitais consagrada neste documento inclui não só meios de pagamento eletrónicos mas também, pela primeira vez, meios de pagamento em moeda virtual.

A propósito de obtenção e preservação da prova digital, especialmente em relação a conteúdos ilegais;

Diretiva 2000/31/CE – **Relativa ao comércio eletrónico**[55]. De entre as várias finalidades da Diretiva, destacamos aquelas que são referentes aos prestadores de serviços. Para efeitos da diretiva, a atividade exercida pelo prestador de serviços limita-se ao processo técnico de exploração e abertura do acesso a uma rede de comunicação na qual as informações prestadas por terceiros são transmitidas ou temporariamente armazenadas com o propósito exclusivo de tornar a transmissão mais eficaz.

[52] Diretiva 2012/29/UE do Parlamento Europeu e do Conselho de 25 de outubro de 2012, que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade e que substitui a Decisão-Quadro 2001/220/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX-:32012L0029&from=en.

[53] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX-:32013L0040&from=DE.

[54] Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019L0713&from=PT.

[55] Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico»), https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX-:32000L0031&from=EN.

Assim, a atividade do prestador de serviço é vista como uma atividade puramente técnica, automática e de natureza passiva, o que implica que o prestador de serviços da sociedade de informação não tem conhecimento da informação transmitida ou armazenada, nem o controlo desta.

Neste sentido, a diretiva prevê um regime geral de irresponsabilidade do prestador de serviço pelo conteúdo ilícito partilhado pelos utilizadores do serviço. Assim, o prestador de serviço não tem o dever de fiscalizar os conteúdos e, por isso, não poderá ser responsabilizado pelos mesmos. Contudo, a isenção de responsabilidade é limitada por um dever de atuar – por via de bloqueio ou remoção dos conteúdos - quando tenha conhecimento de que os destinatários dos seus serviços estão a utilizar o mesmo para armazenar conteúdo ilegal. Nestes casos, o prestador de serviço deve, assim que tenha conhecimento ou que lhe seja dado conhecimento, o dever de proceder com diligência no sentido de remover as informações ou impossibilitar o acesso a estas. Ao prestador de serviço não é exigido uma vigilância ativa de conteúdos ilegais, no entanto é possível aos Estados Membros legislar no sentido de definir certos deveres de diligência aos prestadores de serviços, no sentido de detetarem e prevenirem determinados tipos de atividades ilegais.[56]

Regulamento 679/2016 – **Implementou o regulamento geral de proteção de dados pessoais (RGPD)** em 2016.[57] Este novo quadro legal vem trazer proteções reforçadas relativamente a dados pessoais. Exclui-se do seu âmbito de aplicação o tratamento de informação para finalidades de prevenção, investigação, deteção ou repressão de infrações penais pelas entidades competentes.[58] Assim, aplica-se a todas as restantes situações que envolvam o processamento de dados pessoais, nomeadamente no caso de deteção de conteúdos ilícitos no âmbito do tratamento de dados por prestador de serviço ou outra entidade, no exercício da sua atividade, uma vez que a finalidade do tratamento dos dados não era a deteção. O RGPD é ainda, assim, aplicável nos casos em que um organismo ou uma entidade recolhe dados pessoais na prossecução da sua atividade e, em seguida, os trata a fim de dar cumprimento a uma obrigação legal a que está sujeito,[59] por exemplo, a remoção de conteúdos de abuso e exploração sexual de menores ou no caso das instituições financeiras quando retêm, para efeitos de investigação, deteção ou repressão de infrações penais, certos dados pessoais por si tratados e os fornecem apenas às autoridades nacionais competentes.

De entre as várias disposições do RGPD, o direito ao esquecimento, consagrado no art.º 17.º deste diploma, ganha maior relevo no que diz respeito à salvaguarda dos direitos das vítimas, principalmente quando os dados pessoais forem tratados de forma ilícita e por isso virem a originar outros danos. Veja-se, a este título, casos de violência doméstica em que numa relação íntima são divulgados imagens ou vídeos íntimos de companheiro/a sem o consentimento deste/a, e disponibilizados em *website* pornográfico. O direito ao esquecimento permite à vítima desta divulgação não consensual de vídeos exigir que a plataforma retire de forma imediata o conteúdo ilícito.

O direito de ser esquecido proporciona ao seu titular a possibilidade de **solicitar verbalmente ou por escrito** que o responsável pelo tratamento de dados apague os dados pessoais do titular do direito. As circunstâncias em que este direito pode ser exercido estão descritas no próprio artigo 17.º.

[56] Ver também a este respeito, Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content *online*, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334&from=EN.

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

[58] Cf. Art. 2/2/d) RGPD. Nestes casos, aplicar-se-á o regime especial da Diretiva 2016/680, transposta pela Lei n.º 59/2019.

[59] Cf Art. 6/1/c) RGPD.

É importante ter em conta que o tratamento ilícito dos dados pessoais, seja pelo encarregado de proteção de dados ou por outras pessoas/entidades não autorizadas ao tratamento desses dados acarreta responsabilidade penal em determinados casos.[60]

Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças[61] - o mais recente documento da UE sobre abuso e exploração sexual de crianças. Esta Comunicação apresenta uma resposta forte e integrada a estes crimes, tanto na sua forma *online* como *offline*. Com vista ao combate destes crimes, a estratégia estabelece oito iniciativas para desenvolver um quadro jurídico adequado, reforçar a resposta dos órgãos de polícia criminal e promover uma ação coordenada entre múltiplos intervenientes no que diz respeito à prevenção, investigação e assistência às vítimas, e define ações específicas a serem tomadas pelos Estados Membros. Além disso, a estratégia compromete a UE à possível criação de um centro europeu para prevenir e combater o abuso sexual de crianças, que prestaria apoio aos Estados-Membros na luta contra o abuso e exploração sexual de crianças, assegurando a máxima coordenação. Esta estratégia deverá ser implementada ao longo dos próximos cinco anos (2020-2025).

A nível Europeu existem ainda Instituições que foram criadas para auxiliar os Estados Membros no combate ao cibercrime, nomeadamente, a *European Union Agency for Network and Information Security* (ENISA) que apoia o intercâmbio de boas práticas a nível de cibersegurança entre os Estados-Membros da UE. Em 2013, dentro da Europol foi criado um departamento específico de combate ao cibercrime – European Cibercrime Centre (EC3) para reforçar a resposta das autoridades policiais dentro da União Europeia. A EC3 atua prestando apoio às polícias dos Estados Membros na luta contra o cibercrime na União Europeia, reunindo a sua experiência no apoio às investigações de crimes informáticos que possam estar a ocorrer nos Estados-Membros.

Para além desta iniciativa, em 2012 foi lançada A Aliança Global Contra o Abuso Sexual de Crianças *Online* pela Comissão Europeia e pelos Estados Unidos da América tendo como objetivo unir esforços em todo o mundo para combater de forma mais eficaz os crimes sexuais *online* contra crianças. Reunindo 54 países, que se comprometeram a adotar ações concretas para melhorar a proteção das vítimas, identificar e agir criminalmente contra os agressores, aumentar a consciencialização e reduzir a divulgação de pornografia infantil *online* e a vitimização de crianças.

A nível internacional cumpre também destacar o papel da Associação INHOPE cuja missão é prestar apoio na criação e manutenção de HOTLINES dedicas ao combate de abuso sexual de menores *online*. Por sua vez, as HOTLINES atuam a nível nacional em articulação constante com as suas congéneres internacionais, de forma a terem estruturas que permitam o reporte pela sociedade civil de conteúdos de abuso sexual de menores que estejam disponíveis na Internet, tendo as HOTLINES como função última levar à remoção e responsabilização criminal de quem disponibiliza este tipo de conteúdo.

[60] Em Portugal, responsabilidade penal nestes casos prevista na Lei n.º 58/2019, de 08 de Agosto, Art.ºs 46º a 52º.

[61] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, COM(2020) 607 final, Bruxelas 24.7.2020, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0607&from=EN

2.3. O enquadramento jurídico do cibercrime em alguns Estados-Membros da União Europeia

2.3.1. O caso de Portugal

No que à lei nacional diz respeito, o quadro de referência resulta, em primeiro lugar, da Lei nº 109/2009 de 15 de setembro, a Lei do Cibercrime (LC), que transpõe para o nosso ordenamento a Decisão-Quadro 2005/222/JAI (que veio a ser substituída pela Diretiva 2013/40/EU) e adapta o direito interno à Convenção de Budapeste (CCCE).

Esta lei prevê os chamados cibercrimes *strictu sensu*, isto é, aqueles cuja prática depende de um sistema informático, e por isso, ciber-dependentes (*cyber-dependent offenses*). Este conceito de cibercriminalidade *strictu sensu* diz respeito aos crimes que atacam a disponibilidade, o acesso, a integridade, a autenticidade, a confidencialidade, a conservação e a segurança da informação.

Contudo, como veremos de seguida, existem outros crimes que podem ser praticados com recurso a meios eletrónicos, ainda que não exclusivamente, tornando-os assim também parte do fenómeno da cibercriminalidade. Dentro destes, há ainda aqueles em que a lei faz referência expressa ao recurso a meios eletrónicos e outros, em que apesar de não existir referência expressa, podem ainda ser praticados com recurso às tecnologias de informação e comunicação (TIC).

Nas seguintes tabelas analisam-se os tipos legais de crime previstos nos art.ºs 3º a 8º da LC:

Quadro I-2: Lei do Cibercrime

Artigo e epígrafe	Condutas	Natureza	Artigo da CCCE
Art.º 3º - **Falsidade informática**	Introdução, modificação, eliminação ou supressão de dados informáticos com intenção de provocar engano nas relações jurídicas ou interferência, por qualquer outro modo, num tratamento informático de dados, produzindo dados ou documentos falsos, com intenção de que estes sejam considerados ou utilizados para finalidades jurídicas relevantes como se fossem verdadeiros.	Pública	Art.º 7º
Art.º 3, nº 3	Usar documento produzido a partir de dados informáticos que foram objeto dos atos referidos no nº 1 deste artigo ou usar cartão ou outro dispositivo no qual se encontrem registados dados que foram objeto dos atos referidos no nº 1 deste artigo.		
Art.º 4º - **Dano relativo a programas ou outros dados informáticos**	Apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, sem permissão legal ou sem estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele.	Semipública	Art.º 7º
Art.º 4, nº 2	A tentativa é punível.		
Art.º 5º - **Sabotagem informática**	Entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informáticos, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele.	Público	Art.º 5º
Art.º 6º - **Acesso ilegítimo**	Aceder a um sistema informático, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele.	Semipública	Art.º 2º
Art.º 6, nº 5	A tentativa é punível.		
Art.º 7º - **Interceção ilegítima**	Intercetar através de meios técnicos transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele.	Pública	Art.º 3º
Art.º 7, nº 2	A tentativa é punível.		
Art.º 8º - **Reprodução ilegal de programa**	Reproduzir, divulgar ou comunicar, ilegitimamente, ao público, um programa informático protegido por lei.	Pública	
Art.º 8, nº 3	A tentativa é punível.		

Quadro I-3: Lei do Cibercrime – criminalização das condutas de facilitação/auxílio material à prática da conduta principal como crimes autónomos e não como cumplicidade

Artigo e epígrafe	Condutas	Artigo da CCCE
Art.º 3º, nº 4 – **Falsidade informática**	Importar, distribuir, vender ou deter para fins comerciais qualquer dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço de acesso condicionado sobre os quais tenham sido praticadas as ações vedadas pelo nº 2 do artigo - introduzir, modificar, apagar ou suprimir dados registados ou incorporados em cartão bancário de pagamento ou em qualquer outro dispositivo que permita o acesso a sistema ou meio de pagamento, a sistema de comunicações ou a serviço e acesso condicionado, produzindo dados ou documentos falsos, com intenção de que estes sejam considerados ou utilizados para finalidades jurídicas relevantes como se fossem verdadeiros.	Art. 6º, nº 1, als. a] e b]
Art.º 4º, nº 3 - **Dano relativo a programas ou outros dados informáticos**	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas pelo nº 1 do artigo.	
Art.º 5º, nº 2 – **Sabotagem informática**	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas pelo nº 1 do artigo.	
Art.º 6º, nº 2 - **Acesso ilegítimo**	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas pelo nº 1 do artigo.	
Art.º 7º, nº 3 - **Interceção ilegítima**	Ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizada pelo nº 1 do artigo.	

Importa tecer algumas considerações sobre os artigos acima descritos.

O **Artigo 3.º**, relativo à **falsidade informática**, pretende tutelar a segurança das relações jurídicas enquanto interesse público essencial, que cabe ao Estado de Direito assegurar.

Diferencia-se da burla informática, previsto no Art.º 221.º Código Penal (CP), pelo **bem jurídico** que visa assegurar. Assim, enquanto o bem jurídico tutelado no primeiro é a integridade dos sistemas de informação e dados informáticos, no segundo é o património. Além disto, para a falsidade informática exigem-se ainda algumas condutas típicas que diferem da burla informática, como é o caso da **produção de dado ou documento não genuíno com intenção de provocar engano nas relações jurídicas e de usar o documento como verdadeiro**.

De notar que no n.º 2 do artigo se inclui a falsificação de dados informáticos inseridos em cartões SIM (*Subscriber Identity Module*). Trata-se de cartões de plástico que contêm um chip (estrutura semicondutora) onde está gravada a informação digital que permite ao respetivo titular utilizar um apa-

relho de telemóvel para aceder a uma rede de telefonia móvel. O objeto da conduta também podem ser cartões ou outros equipamentos que permitam o acesso a sinal de televisão por cabo, à internet ou a serviços telefónicos - «dispositivos que permitam aceder a serviços de acesso condicionado».

Exemplo: *E-mail* de *Phishing* que reencaminha Josefina para uma página Web desenhada por cibercriminosos/as para parecer igual à da sua entidade bancária com o intuito de levar Josefina a lá colocar a sua informação bancária.

No **art.º 4.º - Dano relativo a programas ou outros dados informático**s, o legislador pretendeu punir **atuações ilegítimas que destruam ou afetem a capacidade de uso de programas ou dados informáticos**. Encontra-se, por isso, excluído do tipo legal testes de segurança a determinado sistema, desde que autorizados pelo dono desse sistema.

O bem jurídico protegido neste tipo de crimes é a integridade e fiabilidade dos dados e o bom funcionamento dos programas informáticos. Ao contrário do crime de dano p. p. no art.º 212 CP, não se pretende apenas proteger a propriedade; o dano informático. Assim, além da integridade patrimonial dos dados informáticos como propriedade do lesado, esta incriminação tutela ainda **a integridade funcional desses dados** no que respeita à **disponibilidade e utilização eficaz dos dados informáticos**. Não exige dolo específico.

Exemplo: O computador do João é infetado com um vírus que lhe deixa o computador muito lento.

O **Artigo 5.º - Sabotagem informática** visa proteger contra **perturbação do funcionamento de sistemas informáticos** ou **perturbação na comunicação de dados**.

A distinção entre o dano informático e a sabotagem informática não é fácil, vejamos; contrapondo os dois tipos de crime podemos dizer que no dano informático se pretende punir atos relacionados com **dados informáticos**, enquanto na **sabotagem o que está em causa é a perturbação do funcionamento normal de sistemas informáticos**. Individualmente considerados, podemos ter atos de dano informático que têm como resultado prático a sabotagem informática devido a afetação do funcionamento de um sistema informático ou de comunicação de dados, sendo que neste caso as **condutas de dano são meramente formas de realização do crime de sabotagem informática**. Por outras palavras, de uma sabotagem informática resultará sempre dano informático.

O tipo legal também pune a difusão de vírus e de outros programas maliciosos, destinados a provocar sabotagem informática (v.g. art.º 5º, n.º 2 da LC). Nestes casos, estamos perante uma antecipação da tutela penal para a fase dos atos preparatórios do crime de sabotagem, por exemplo, a montagem de *botnets* destinados a permitir o controlo malévolo de redes, por via do estabelecimento de uma rede de computadores «*zombie*» cujo uso posterior provocará falhas técnicas conhecidas por *DoS* e *DDoS*.

O **artigo 6.º - Acesso ilegítimo** pretende tutelar a segurança do sistema informático, sobretudo, a

sua confidencialidade. Trata-se de um crime de perigo abstrato destinado a funcionar como barreira para evitar a prática de outros ilícitos de maior gravidade. Assim sendo, para que a conduta típica se verifique basta estar **consumado o acesso não autorizado**, já que a tomada de conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei, configura circunstância agravante do crime de acesso ilegítimo (art.º 6.º, n.º 4 da LC).

Não é exigido dano ou lesão de dados, programas ou sistemas informáticos para se consumar o crime de acesso ilegítimo. Para efeitos da lei, acesso é entrada no todo ou em parte de um sistema informático (*hardware*, componentes, dados armazenados no sistema, diretorias, dados de tráfego e dados relativos ao conteúdo). Contudo, art.º 6.º, n.º 2 não pune a compra/aquisição de dados ou de programas que facilitem o acesso, mas tão só a venda.

Para que o crime seja consumado não é exigido ao autor do crime qualquer intenção específica, basta apenas que o mesmo tenha intenção de aceder ao sistema.

O crime de acesso ilegítimo pode ser cometido através de 1) Acesso realizado com exploração de fragilidades do sistema acedido ou 2) Acesso realizado por pessoa das relações da vítima (ex-namorado, por exemplo), abusando da autorização de acesso que lhe foi concedida.

Exemplos: Comete o crime de acesso ilegítimo alguém que: 1) não estando autorizado para tal, explora uma fragilidade do sistema e acede a grupo privado da plataforma de comunicação Whatsapp® criado por alunos do secundário e; 2) Ana deu a *password* ao namorado para, em determinada data, aceder ao *e-mail* desta e ver se tinha chegado *e-mail* importante. Bem sabendo que esta só o tinha autorizado a aceder ao seu *e-mail* naquele dia, o dito ex-namorado volta a usar a password de Ana para aceder ao *e-mail* desta em momento posterior.

No **artigo 7.º - Interceção ilegítima**, a lei pretendeu tutelar a reserva da vida privada, enquanto direito ao sigilo sobre comunicações de dados informáticos, por via do sigilo em todas as comunicações digitais.

Ficam excluídos do tipo penal as interceções autorizadas por lei (realizadas ao abrigo de normas processuais penais (exemplos: art.º 12.º a 19.º da LC) ou realizadas com autorização ou por ordem dos intervenientes nas transmissões de dados (atividades de teste ou proteção aprovadas pelos participantes).

Constitui crime a interceção de qualquer forma de transferência eletrónica de dados, por telefone, fax, correio eletrónico ou ficheiro. Para a consumação do crime **não se exige a efetiva obtenção de informações**, basta proceder de forma a captar essas informações, já que a tentativa de intercetar é punível.

Exemplo: Pedro Instala Software no telefone de Maria que lhe permite ter acesso a todas as suas comunicações telefónicas.

De notar que os tipos de crime previstos nos artigos 3.º a 7 incluem também, com as mesmas penas,

os atos de produzir, vender, distribuir, disseminar ou introduzir num sistema informático um dispositivo ou programa que permita a prática da conduta tipificada para o crime em questão. Ex: No caso do acesso ilegítimo, será agente do crime de acesso ilegítimo quem, ainda que não tenha acedido ou tentado aceder, produza um programa que permita a terceiros aceder a sistema de uma outra pessoa.

O **artigo 8.º - Reprodução ilegítima de programa protegido** visa proteger um direito privado, um programa informático. Neste sentido, o artigo 14.º do DL 252/94, de 20/10, que regula a proteção jurídica de programas de computador, dispõe expressamente que quanto à tutela penal dos programas de computador lhes é aplicável o disposto no n.º 1 do artigo 9º da LC. Entendeu-se, assim, existir um interesse essencial do Estado em **proteger os criadores intelectuais** e que, por isso, se justificava o interesse do Estado em agir criminalmente contra a violação de direitos desta natureza. Portanto, este crime não depende de queixa, sendo um crime público.

Os arts.º 11º a 19º estabelecem normas relativamente ao direito processual, que permitem a recolha expedita e manutenção de prova eletrónica. Aplicam-se, por isso, aos crimes previstos nesta lei, àqueles que sejam cometidos por meio de um sistema informático ou em relação aos quais seja necessário proceder à recolha de prova em suporte eletrónico.

Os arts.º 20º a 26º relacionam-se com a cooperação internacional e o art.º 27º com a jurisdição territorial.

O Código Penal Português e disposições em matéria de Cibercrime

Como referido anteriormente, no ordenamento jurídico Português, para além da LC, é ainda possível encontrar previsões de crimes cujo cometimento se pode dar com recurso a meios eletrónicos, ainda que não exclusivamente, também chamados de crimes facilitados por sistema informático (*cyber-enabled offenses*).

Em alguns casos a lei prevê expressamente o recurso a esses meios eletrónicos, noutros não, o que não impede que sejam praticados com recurso aos mesmos. No próprio Código Penal (CP) podem ser encontradas algumas incriminações que referem expressamente o recurso a meios eletrónicos para a prática do crime. A tabela que se segue junta as disposições de incriminações que podem facilitadas por sistema informático, a saber:

Quadro I-4: Código Penal Português

Artigo e epígrafe	Condutas	Natureza
Art.º 152º, nº 2, al. b) – **Violência Doméstica**	Difundir através da Internet ou de outros meios de difusão pública generalizada, dados pessoais, designadamente imagem ou som, relativos à intimidade da vida privada de uma das vítimas sem o seu consentimento.	Pública
Art.º 176, nº 1, als. a), b), c) e d) – **Pornografia de menores**	Utilizar menor em espetáculo pornográfico ou o aliciar para este fim; utilizar menor em fotografia, filme ou gravação pornográficos ou, independentemente do seu suporte, ou o aliciar para esse fim; produzir, distribuir, importar, exportar, divulgar, exibir, ceder ou disponibilizar os materiais previstos na alínea anterior; adquirir, detiver ou alojar aqueles materiais com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder.	Pública
Art.º 176, nº 5	Adquirir, detiver, aceder, obtiver ou facilitar o acesso, através de sistema informático ou qualquer outro meio aos materiais referidos na alínea b).	
Art.º 176, nº 6	Presencialmente ou através de sistema informático ou qualquer outro meio, assistir, facilitar ou disponibilizar acesso a espetáculo pornográfico envolvendo a participação de menores de 16 anos de idade.	
Art.º 176, nº 8	Considera-se pornográfico todo o material que, com fins sexuais, represente menores envolvidos em comportamentos sexualmente explícitos, reais ou simulados, ou contenha qualquer representação dos seus órgãos sexuais ou de outra parte do seu corpo.	
Art.º 176, nº 9	A tentativa é punível.	
Art.º 176 – A – **Aliciamento de menores**	Aliciamento de menor, por meio de tecnologias de informação e de comunicação, para encontro visando a prática de atos de abuso sexual de menores ou atos de pornografia infantil.	Pública
Art.º 193º - **Devassa por meio de informática**	Criar, manter ou utilizar ficheiro de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou à origem étnica.	Pública
Art.º 193, nº 2	A tentativa é punível.	
Art.º 221º - **Burla informática e nas comunicações**	Interferir no resultado de tratamento de dados ou estruturar incorretamente programa informático, utilizar incompleta ou incorretamente dados, a utilizar dados ou intervir por qualquer modo no processamento, sem autorização, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causando a outra pessoa prejuízo patrimonial.	Semipública
Art.º 221, nº 2	Causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.	
Art.º 221, nº 3	A tentativa é punível.	
Crimes que, pesa embora não exista menção expressa de recurso a meios eletrónicos, são hoje em dia, maioritariamente, praticados por via daqueles;		
Art.º 154-A - Perseguição	Perseguir ou assediar outra pessoa, por qualquer meio, direta ou indiretamente, de modo reiterado, de forma adequada a provocar-lhe medo ou inquietação ou a	Semipública

	prejudicar a sua liberdade de determinação.	
Art.º 154-A , nº 2	A tentativa é punível.	
Art.º 192º - **Devassa da vida privada**	Intercetar, gravar, registar, utilizar, transmitir ou divulgar uma conversa, uma comunicação telefónica, mensagens de correio eletrónico ou faturação detalhada; captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objetos ou espaços íntimos; observar ou escutar às ocultas pessoas que se encontrem em lugar privado ou divulgar factos relativos à vida privada ou a doença grave da vítima, sem consentimento da vítima e com intenção de devassar a vida privada desta, nomeadamente a sua intimidade familiar ou sexual.	Semipública
Art.º 194 - **Violação de correspondência ou de telecomunicações**	Abrir uma encomenda, uma carta ou qualquer outro escrito que se encontre fechado e que não lhe seja dirigido, ou tomar conhecimento, por processos técnicos, do seu conteúdo, ou impedir, por qualquer modo, que seja recebido pelo destinatário; intromissão no conteúdo das telecomunicações ou tomar conhecimento das mesmas e divulgar o conteúdo de escritos fechados ou telecomunicações.	Semipública
Art.º 199.º - **Gravações e fotografias ilícitas**	Sem consentimento, gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; utilizar ou permitir que se utilizem as gravações referidas, mesmo que licitamente produzidas; fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado ou utilizar ou permitir que se utilizem fotografias ou filmes já referidos, mesmo que licitamente obtidos.	Semipública
Art.º 199.º, n.º 2, b)	Divulgação de imagens não consentida.	
Art.º 240.º, n.º 1, al. a) e b) - **Discriminação e incitamento ao ódio e à violência**	Fundar ou constituir organização ou desenvolver atividades de propaganda organizada que incitem à discriminação, ao ódio ou à violência contra pessoa ou grupo de pessoas por causa da sua raça, cor, origem étnica ou nacional, ascendência, religião, sexo, orientação sexual, identidade de género ou deficiência física ou psíquica, ou que a encorajem; ou participar na organização ou nas atividades referidas na alínea anterior ou lhes prestar assistência, incluindo o seu financiamento.	Pública
Art.º 240.º, nº 2, al) a	Através de apologia, negação ou banalização grosseira de crimes de genocídio, guerra ou contra a paz e a humanidade, publicamente, por qualquer meio destinado a divulgação, provocar atos de violência, difamar ou injuriar, ameaçar ou incitar à violência ou ao ódio, contra as pessoas referidas no n.º1.	
Artigo 223.º - **Extorsão**	Constranger outra pessoa, com intenção de conseguir para si ou para terceiro enriquecimento ilegítimo, por meio de violência ou de ameaça com mal importante, a uma disposição patrimonial que acarrete prejuízo para essa pessoa ou para outrem.	Pública
Artigo 223.º , n.º 2	Quando a ameaça consistir na revelação, por meio da comunicação social, de factos que possam lesar gravemente a reputação da vítima ou de outra pessoa.	

O preceito no **artigo 152.º, n.º 2, al. b) - Violência Doméstica** foi introduzido pela Lei n.º 44/2018. Com este novo preceito visa proteger-se particularmente os dados pessoais (designadamente imagem ou som, o que inclui vídeos, filmes, fotos) sobre a intimidade (nomeadamente a sexualidade) e a reserva da vida privada de qualquer vítima quando difundidos (divulgados/espalhados) através da Internet ou de outros meios de difusão pública generalizada (como, por exemplo, através das

redes sociais), sem o consentimento da vítima. Esta incriminação visou censurar de forma acrescida, através desta qualificação especial, o *ciber-stalking* em contexto de violência doméstica (entendido este como as condutas que consistem sobretudo, como diz Carolina Villacampa Estiarte, em "enviar correios eletrónicos, mensagens de texto e mensagens instantâneas ofensivas ou ameaçadoras, publicar comentários ofensivos sobre a vítima na internet, partilhar fotografias ou vídeos íntimos da mesma através da internet", que são vividas como "mais intrusivas para as vítimas" e que lhes "provocam mais efeitos psicológicos adversos").

Relativamente ao **artigo 176.º - Pornografia de menores**, os atos materiais nele tipificados vão além dos descritos na Diretiva 2011/93/EU, apesar de ficarem atrás da Convenção de Lanzarote. Neste sentido, deve notar-se a Lei 40/2020 de 18 de Agosto que veio alterar algumas alíneas deste artigo, assim como aditou ao CP o artigo 176.º-B referente a organização de viagens para fins de turismo sexual com menores.

O **artigo 176.º - A - Aliciamento de menores para fins sexuais** foi adicionado ao CP pela Lei n.º 103/2015, de 24 de agosto. Deste modo, cumprindo os ensejos da Diretiva 2011/93/ EU, passaram a ser criminalizadas novas formas de abuso e de exploração sexual facilitadas pela utilização das TIC, como por exemplo o aliciamento de menor através da internet, os espetáculos pornográficos em tempo real na internet, ou o acesso, com conhecimento de causa e intencionalidade, à pornografia infantil alojada em determinados sítios da Internet.

O **artigo 193.º - Devassa por meio de informática**, decorre do preceito constitucional previsto no artigo 35º n.º 3 da Constituição da República Portuguesa, e visa proteger a reserva da vida privada contra possíveis atos de discriminação que a utilização de meios informáticos torna exponencialmente perigosos. Razão pela qual o procedimento criminal relativamente ao crime previsto neste artigo 193º não depende de queixa. É assim, um crime público, sobre o qual o Estado terá sempre interesse e dever de agir. No tipo legal da devassa por meio de informática encontramos não só os atos de criação de ficheiros violadores do bem protegido, mas também os meros atos de conservação e utilização desse ficheiro, ainda que sem qualquer comparticipação na sua criação. O tipo legal é, desta forma, bastante abrangente quanto às condutas penalizadas, o que pretende ser um facto dissuasor face à dificuldade de prova quanto ao autor material do ficheiro. No mesmo sentido se penaliza a mera tentativa.

A incriminação da **burla informática e nas comunicações** prevista no **artigo 221º** surge no desenvolvimento da disciplina geral da burla, comungando dos mesmos elementos delimitadores do tipo do art.º 217º do CP; a intenção de obter para si ou para terceiro enriquecimento ilegítimo e o requisito de causar a terceiro prejuízo patrimonial. Tal como no tipo geral da burla, a tentativa é punível e o procedimento penal depende de queixa. A **especificidade deste tipo** legal está no processo utilizado: **a utilização de meios informáticos**, ou seja, a utilização de meios informáticos de forma ardilosa para manipulação de dados ou de resultados. O n.º 1 do artigo refere-se à interferência no resultado de tratamento de dados com vista a obter um benefício ilegítimo, enquanto o n.º 2 diz respeito à utilização de meios informáticos com o intuito de perturbar a integridade/normal funcionamento dos sistemas informáticos, com vista à obtenção de vantagem ilegítima.

Passa-se agora a uma análise de crimes que, apesar de não preverem expressamente o recurso a meios informáticos, existe uma grande probabilidade que, face ao aumento exponencial do acesso à internet e a *smartphones*, sejam praticados com recurso aos mesmos;

O **artigo 194.º - Violação de correspondência ou de telecomunicações**, encontra-se abrangido pela agravação caso os conteúdos sejam difundidos através da internet (cf. art.º 197.º CP). Este artigo decorre do direito fundamental previsto no art.º 34.º da Constituição da República Portuguesa que consagra a inviolabilidade das comunicações, tipificando como crime a conduta de violação daquelas. É diretamente aplicável à correspondência eletrónica (via *e-mail*) e todas as demais comunicações eletrónicas e por serviços de telefone móveis (SMS, etc.) que são modernamente equiparáveis à correspondência postal fechada. Os bens protegidos neste preceito são a privacidade, a proteção da liberdade de expressão e a confiança da comunidade na integridade dos meios de comunicação, nomeadamente das telecomunicações e a segurança.

A proteção compreende tanto o conteúdo das comunicações eletrónicas como as circunstâncias da comunicação (dados de tráfego). A simples conservação de dados já configura por si uma violação, que se repete em cada nova utilização ou aproveitamento do conteúdo dos dados de tráfego. Nas comunicações eletrónicas, para verificação do tipo não se exige a tomada de conhecimento do conteúdo mas tão só o acesso é suficiente (já que não é necessário a "abertura").

Coloca-se a questão de saber se este crime não se encontra absorvido pelo crime de "interceção ilegítima", previsto pelo artigo 7º da Lei 109/91. Parece-nos que, embora possa existir sobreposição quando a interceção da mensagem se dá durante a sua transmissão, já não haverá quando o acesso à mensagem se dá depois de esta ter sido já rececionada pelo seu destinatário, encontrando-se guardada na sua caixa de correio eletrónico. Embora, neste último caso, também se pudesse afirmar que estamos perante um crime de "acesso ilegítimo" previsto pelo artigo 6º da LC, entendemos não ser o caso, desde logo porque este crime exige uma **especial intenção: "intenção de alcançar, para si ou para outrem, um benefício ou vantagem ilegítimos"**, que o crime de "violação de correspondência ou de telecomunicações" não exige. Não se justificaria, assim, que uma correspondência fechada eletrónica, depois de rececionada, ficasse menos protegida que a correspondência em papel. Entendemos por isso que este crime se aplica ainda à correspondência eletrónica.

Ainda sob a alçada da perturbação da privacidade ou da vida privada, encontram-se as seguintes incriminações; **violação de domicílio ou perturbação da vida privada** (art.º 190 CP), **introdução em lugar vedado ao público** (191.º CP), **devassa da vida privada** (arts.º 192º CP), **violação de segredo** (art.º 195.º CP). Em todas está prevista agravação se os conteúdos forem difundidos através da internet, cf. art.º 197.º CP).

A gravação e fotografias ilícitas prevista no **art. 199º CP** pretende salvaguardar o direito à imagem que constitui um bem jurídico-penal autónomo tutelado em si e independentemente do ponto de vista da privacidade ou intimidade retratada. O direito à imagem abrange dois direitos autónomos: o

direito a não ser fotografado e o direito a não ver divulgada a fotografia. O visado pode autorizar ou consentir que lhe seja tirada uma fotografia e pode não autorizar que essa fotografia seja usada ou divulgada. Contra vontade do visado não pode ser fotografado nem ser usada uma sua fotografia.

Exemplo: João, contra a vontade da Maria, utiliza uma fotografia desta, ainda que licitamente obtida – a Maria havia consentido em ser fotografada - e a publica no Facebook®.

Para além destes tipos, outros crimes comuns podem ser praticados e os seus efeitos potenciados fazendo uso das tecnologias. **São crimes cujo tipo não contempla como elemento constitutivo do crime a utilização do meio tecnológico**.

O crime de **perseguição**, previsto no **art.º 154-A**, poderá ser passível de ser praticado com recurso a meios eletrónicos, vulgo *ciber-stalking*. Devido á sua tendência duradoura e que tende, em muitos casos, a tornar-se mais grave com o decurso do tempo, o crime de *stalking* poderá integrar outros tipos de crime, e.g. art.º 193 CP que prevê a devassa por meios informáticos, crime de gravação e fotografias ilícitas previsto no art.º 199º CP.[62] Também o crime de **discriminação e incitamento ao ódio e à violência**, previsto no **artigo 240.º**, poderá ser cometido por via de meios eletrónicos.

O crime de Extorsão, previsto no artigo 223.º do CP está, normalmente, associado às práticas de *ransomware*. Com efeito, normalmente associado ao bloqueio de um determinado sistema, pela encriptação dos dados nele armazenados ou dos respetivos ficheiros operativos, vem comunicação exigindo, em troca do seu desbloqueio, elevada quantia (normalmente, a ser paga em *Bitcoins*).

Outros exemplos: Crimes contra a honra cometidos através da inclusão das expressões ou acusações injuriosas em páginas *online*, blogs ou difundindo-as por correio eletrónico. A única relevância do meio eletrónico respeita à utilização desse meio para a divulgação da expressão injuriosa ou difamatória e à superior potencialidade de dano para o bem jurídico protegido (cf. Art.º 183º/1 a) CP: ofensa praticada através de meios que facilitem a sua divulgação; e n.º 3 CP: meio de comunicação social, v.g. redes sociais).

O **Decreto-lei n.º 7/2004, de 07 de Janeiro** transpôs a Diretiva 2000/31/CE. Assim, é neste instrumento estabelecido o princípio da irresponsabilidade dos prestadores intermediários de serviços em rede face à eventual ilicitude das mensagens que disponibilizam. Neste sentido, parte-se da declaração de ausência de um dever geral de vigilância do prestador intermediário de serviços sobre as informações que transmite ou armazena ou a que faculte o acesso (art.º 12.º), para uma obrigação de informação/comunicação imediata ao Ministério Público sempre que tenham conhecimento que a disponibilização de conteúdos por meio dos serviços que prestam, ou o acesso aos mesmos, possa constituir crime (art.º 13.º a)).[63] A mais recente alteração introduzida pela Lei 40/2020 de 18 de Agosto vem estender este dever de informação e reforçá-lo para qualquer caso de deteção de conteúdos por si disponibilizados que possa constituir crime, nomeadamente crime de pornografia de menores ou crime de discriminação e incitamento ao ódio e à violência.[64]

[62] Cibercrime e *Stalking*, Vânia Costa Ramos, p. 11. https://carlospintodeabreu.com/public/files/cibercrime_stalking.pdf

[63] Não especialmente relevante para a perspectiva do apoio à vítimas, mas relevante como exemplo de como a intervenção dos ISP's pode ocorrer, veja-se o Memorando de Entendimento celebrado entre a IGAC (Inspeção Geral das Atividades Culturais), os ISP's e as associações representantes de titulares de propriedade intelectual, com vista a facilitar a identificação e remoção/bloqueio de páginas que divulguem conteúdos manifestamente violadores de direitos de autores. Cf. http://www.apel.pt/gest_cnt_upload/editor/File/apel/direitos_autor/memorando_APRITEL_IGAG_MAPINET.pdf

[64] Ver novíssimo artigo 19.º - A do DL n.º 7/2004, aditado pela Lei 40/2020 de 18 de Agosto.

Para além deste dever de comunicação às autoridades, incube também aos Prestadores Intermediários de Serviços, nos casos em que toma conhecimento – por si ou através de terceiros – da existência de conteúdo de natureza **manifestamente** ilegal, proceder ao bloqueio ou remoção dos mesmos (cf. art.ºs 13.º c); art.º 15.º, nº 3; art.º 16.º, nº1; art.º 17.º). Com as alterações introduzidas pela Lei 40/2020 de 18 de Agosto, os Prestadores estão obrigados à remoção, num prazo de 48 horas, de conteúdos de abuso ou exploração sexual de menores.[65]

O desrespeito pelos deveres específicos de informação e bloqueio dão lugar à responsabilização dos Prestadores Intermediários de Serviços, seja através do mecanismo da Responsabilidade Civil (art.º 16) ou através da aplicação de Contraordenações (art.º 37) pela entidade responsável pela Supervisão - ANACOM.

A **Lei n.º 32/2008, de 17 de Julho**, conhecida como a lei da retenção de dados (LRD) no contexto de oferta de serviços de comunicações eletrónicas para fins de investigação, deteção e repressão de crimes graves por parte das autoridades competentes, veio transpor a Diretiva 2006/24/CE, que entretanto já não se encontra em vigor no direito da UE.[66] Contudo, aquela lei vigora ainda no ordenamento jurídico português. As disposições mais relevantes em matéria de conservação da prova digital encontram-se no artigo 4.º, n.º 3 que define o que são crimes graves para os efeitos desta lei, apresentando assim um catálogo de crimes cuja investigação permitirá o recurso a dados retidos por prestadores de serviço e o artigo 6.º, onde se prevê o **prazo de um ano para armazenamento dos dados de tráfego e localização** no setor das comunicações eletrónicas.

Por fim, a **Lei n.º 46/2018, de 13 de Agosto** que estabelece o **Regime Jurídico da Segurança do Ciberespaço**, transpondo a Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União,[67] veio criar o Conselho Superior de Segurança do Ciberespaço (CSSC), como órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço. Nos art.ºs 5.º e 6.º a lei define as competências do CSSC e no art.º 7.º define as competências do Centro Nacional de Cibersegurança (CNCS). Nos art.ºs 8.º e 9.º enquadra legalmente a Equipa de Resposta a Incidentes de Segurança Informática Nacional – CERT.PT – e define as suas competências, integrada no CNSC. Esta lei estabelece ainda requisitos mínimos de cibersegurança e obrigações de comunicação de incidentes a todos os níveis governamentais e entidades públicas, prestadores de serviço de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais, perante o CNCS que, posteriormente, informa, caso haja lugar, os pontos de contacto de outros Estados Membros afetados.

Em 12 de junho de 2019, o Governo adotou a **Resolução do Conselho de Ministros n.º 92/2019 que aprovou a primeira Estratégia Nacional de Segurança do Ciberespaço**, visando aprofundar a segurança das redes e dos sistemas de informação e potenciar uma utilização livre, segura e eficiente do ciberespaço, por parte de todos os cidadãos e das entidades públicas e privadas. A estratégia baseia-se em três princípios: subsidiariedade da intervenção estatal, complementaridade da atuação (estreita ligação e coordenação com diversos atores) e proporcionalidade (na alocação de recursos e serviços para fazer face às ameaças digitais).

[65] Ver artigo 19.º - B do DL n.º 7/2004, aditado pela Lei 40/2020 de 18 de Agosto, que obriga expressamente à remoção, num prazo de 48 horas, de conteúdos de abuso ou exploração sexual de menores.

[66] https://eur-lex.europa.eu/eli/dir/2006/24/oj/por

[67] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

2.3.2. O caso da Roménia

O ordenamento jurídico Romeno não dispõe de lei especial sobre o cibercrime. Neste sentido, os dispositivos legais de incriminação encontram-se previstos no Código Penal Romeno, em dois títulos distintos, a saber:

Título II – Crimes contra o património
Capítulo IV – Burla através de sistemas informáticos ou meios de pagamento eletrónicos:

- Burla informática (Art.º 249), definida como a conduta de "introduzir, modificar ou apagar dados informáticos, restringir o acesso a estes dados ou, de qualquer outra forma, impedir o normal funcionamento do sistema informático, com vista a obtenção de vantagem patrimonial, da qual resulte dano";
- Realização de transações financeiras fraudulentas (Art.º 250) – "executar operações de levantamento de dinheiro, depósito ou descarregamento de instrumentos de pagamento eletrónico ou transferência de fundos através do recurso a meios de pagamento eletrónicos sem o consentimento do proprietário ou a dados que permitam a sua identificação";
- Aceitação de transações financeiras fraudulentas (Art.º 251) – "aceitação das transações supracitadas em pleno conhecimento da sua natureza fraudulenta";

Título VII – Crimes contra a segurança pública
Capítulo VI – Crimes contra a segurança e integridade de sistemas e dados informáticos

- Acesso ilegítimo a sistema informático (Art.º 360), que diferencia o acesso ilegítimo a um sistema informático, do acesso ilegítimo a sistema informático com o propósito de obter dados informáticos, e do acesso ilegítimo a sistema informático que tem programas, dispositivos ou procedimentos que restringem o acesso ao mesmo. Aos três tipos de crime correspondem sanções gradualmente mais severas;
- Interceção ilegítima de dados processados eletronicamente (Art.º 361)
- Alteração da integridade de dados informáticos (Art.º 362) – "ilegitimamente modificar, apagar, deteriorar ou danificar dados informáticos ou restringir acesso aos mesmos";
- Perturbação do funcionamento de sistemas informáticos (Art.º 363) - "perturbação grave, sem autorização, do funcionamento de sistema informático, sob a forma de introduzir, transmitir, modificar, apagar ou deteriorar dados informáticos ou restringir o acesso aos mesmos";
- Transferência não autorizada de dados informáticos (Art.º 364)
- Operações ilegais em dispositivos informáticos ou *softwares* (Art.º 365) – "produzir, importar, distribuir, fornecer ou ilegitimamente possuir dispositivos, programas, palavras-passe e códigos de acesso que permitam acesso total ou parcial a sistema informático com o propósito de cometer os crimes previstos nos Artigos 360 a 364.

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

- Pornografia infantil (Art.º 374), definido como a conduta de "produzir, possuir, obter, conservar, expor, promover, disseminar ou divulgar, e/ou fornecer, de qualquer forma, conteúdos pornográficos referentes a menores, bem como extorquir ou recrutar menores com o propósito de participar em espetáculo pornográfico, obtendo daí vantagem, ou explorar menores de qualquer outra forma para a realização de espetáculo pornográfico." A visualização de conteúdos pornográficos referentes a menores também é punida por lei. A componente de cibercriminalidade na pornografia infantil é evidente no parágrafo 2 do Artigo 374, na parte em que menciona expressamente as sanções para as condutas supracitadas, sejam elas cometidas através de sistema informático ou qualquer outro meio de comunicações eletrónicas. Além disso, o parágrafo 4 expressamente inclui novas tecnologias de informação e comunicação como meios de comunicação para espetáculos pornográficos.

A tentativa de cometer qualquer das condutas acima referidas é punida, de acordo com o disposto nos Artigos 252, 366 e 374 (5) do Código Penal Romeno.

O compromisso do país no combate à cibercriminalidade foi reforçado em 2011, aquando da criação, pelo Governo, da Equipa Nacional de Resposta a Incidentes de Segurança Informáticos (em Romeno: *Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică* – CERT-RO), que consiste num centro independente e especializado de pesquisa, investigação e desenvolvimento em cibersegurança. Em 2013, a Roménia aprovou a Estratégia Nacional para a Cibersegurança, que visou também a criação de um Sistema Nacional para a Cibersegurança (Em Romeno: *Sistemul naţional de securitate cibernetică* - SNSC), que se baseia num enquadramento geral em matéria de cooperação transversal entre autoridades públicas e instituições ou representantes da indústria.

Em Julho de 2020, a Lei 217/ 2003 sobre a prevenção e combate à violência doméstica foi alterada e a violência cibernética foi incluída entre as formas reconhecidas de violência doméstica, a par da violência verbal, física, sexual, psicológica, económica, espiritual, e social. De acordo com a Lei 217/ 2003, a violência cibernética é definida como "assédio *online*, discurso de ódio *online*, perseguição *online*, ameaças *online*, publicação não consensual de informação e conteúdo gráfico íntimo, acesso ilegal à interceção de comunicações e dados privados e qualquer outra forma de utilização abusiva das tecnologias de informação e comunicações através de computadores, *smartphones* ou outros dispositivos semelhantes que utilizem telecomunicações ou se liguem à Internet e possam transmitir e utilizar plataformas sociais ou de correio eletrónico com o objetivo de confranger/envergonhar, humilhar, intimidar, ameaçar ou silenciar a vítima".[68] É importante notar que estas disposições se referem a ações ou inações intencionais que incluem qualquer das formas de violência acima mencionadas e que ocorrem "num ambiente doméstico ou familiar, entre cônjuges ex-cônjuges, entre parceiros ou ex-companheiros, independentemente de o agressor residir ou ter residido com a vítima" (Art.º 3.º).

Por último, ao momento da conclusão do atual Manual, encontra-se para análise, no Parlamento romeno, uma proposta para sancionar a pornografia não consensual (ou a chamada "pornografia de vingança/*revenge porn*"[69]), adotada pelo Senado a 21 de Outubro de 2019, e posteriormente enviada à Câmara dos Deputados para debate. A proposta procura alterar o artigo 226 do Código Penal (que

[68] Artigo 4 (h) da Lei 217/ 2003, alterada pela Lei n.º 106 de 3 de Julho de 2020.

[69] O autor desaconselha a utilização do termo "pornografia de vingança", uma vez que isto implica que a vítima está em falta e o agente do crime está a divulgar o material como forma de punição. Além disso, "pornografia" implica material produzido para um público mais vasto e/ou para suscitar excitação sexual, enquanto, em muitos destes crimes, o objetivo é principalmente controlar e abusar das vítimas. Portanto, a terminologia preferida é "distribuição não consensual de material sexual".

prevê a incriminação da violação da vida privada), de modo a incluir a incriminação de pornografia não consensual, tipificando, para tal, as condutas de "partilha, apresentação ou transmissão de imagens íntimas, independentemente dos meios utilizados, de uma pessoa sem o seu consentimento", cuja prática poderá acarretar pena de prisão entre 3 meses a 2 anos ou multa.[70]

2.3.3. O caso da Alemanha

Com a entrada em vigor da Convenção de Lanzarote e da Convenção de Budapeste, a legislação penal alemã foi adaptada no sentido de incorporar os recentes desenvolvimentos em matéria de internet e crimes informáticos. Subsequentemente, a legislação alemã incorporou também importantes diretivas da EU em matéria de ataques cibernéticos e de proteção de crianças contra o abuso e exploração sexual de menores e pornografia infantil. Importantes alterações foram a tipificação penal da conduta de aliciamento de menores e a alteração da medida das penas de acordo com a Convenção de Lanzarote.

A **BKA** (Departamento Criminal da Polícia Federal) é a **autoridade pública** responsável em **matéria de cibercriminalidade**, tanto a nível interno como em cooperação internacional, especialmente nas áreas de burla de cartões *online*. A BKA também trabalha diretamente no combate ao cibercrime ao lado de agências como a Interpol e a Europol.

O Ministério da Administração Interna tem vindo a desenvolver estratégias nacionais de combate à cibercriminalidade, reforço da segurança em telecomunicações e sistemas informáticos e melhoria da proteção concedida aos utilizadores da internet na Alemanha.[71] A primeira entrou em vigor em 2011 e ainda hoje os seus objetivos são, em grande medida, aplicáveis. No entanto, a rápida evolução do fenómeno tornou necessário, em 2016, complementá-los e agrupá-los numa nova estratégia que cruza serviços de modo transversal com vista a promover e agilizar cooperação entre diferentes partes interessadas, tendo em conta a natureza transsetorial da cibercriminalidade.[72]

Relativamente aos diplomas legais relativos ao combate ao cibercrime, partindo do preceito constitucional que prevê a inviolabilidade das telecomunicações, passando pelos dispositivos em matéria de crime previstos no Código Penal Alemão e terminando em legislação avulsa como é o caso da **Lei das telecomunicações (TKG), Lei de serviços de informação e comunicação eletrónicos (TMG), Lei de segurança informática (IT-Sicherheitsgesetz)** e **Lei do *Facebook* (NetzDG)**, o ordenamento jurídico alemão aparenta estar legalmente bem equipado para combater esta realidade dinâmica e transfronteiriça que é o cibercrime, apostando numa forte cooperação nacional com entidades privadas da indústria.

O mesmo se dirá da **Lei de Protecção da Juventude (JuSchG)** que visa reforçar e proteger as crianças e os jovens, restringindo o acesso a produtos perigosos para a saúde, a filmes cinematográficos e meios de comunicação com suporte de imagem e visitas a certos websites de domínio público a certos grupos etários. Está atualmente em curso uma discussão para que a lei seja alterada com enfoque na prevenção do aliciamento e assédio online.

[70] Para mais informações sobre a proposta de lei sobre pornografia não consensual, consultar https://www.senat.ro/legis/lista.aspx?nr_cls=L512&an_cls=2019.

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

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

Assim, o **Artigo 10 da Constituição Alemã** prevê a inviolabilidade do sigilo da correspondência, postal e de telecomunicações.

No que toca à lei penal, o **Código Penal Alemão (StGB)** reúne em si as principais incriminações referentes à cibercriminalidade, não existindo, ao contrário do caso do ordenamento jurídico Português, fragmentação entre a lei penal geral e a lei do cibercrime.

Desta feita, o **StGB** prevê três tipos de ilícitos penais relacionados com cibercrime:

Aqueles cujo tipo prevê uma conduta respeitante ao **uso ilegítimo de sistemas ou dados informáticos**, particularmente relacionados com ciber-ataques:

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

Artigo e epígrafe	Condutas	Artigo da CCCE
§ 202a – **Espionagem de dados informáticos**	Obter acesso não autorizado a dados transmitidos eletronicamente (ou a um sistema de informação) não destinados a si ou acesso não autorizado a dados especialmente protegidos, ultrapassando mecanismos de segurança (e.g. encriptação).	2
§ 202b – **Interceção de dados informáticos**	Obter dados cujo acesso não é autorizado a partir de uma transmissão de dados não pública ou da radiação eletromagnética de um sistema de tratamento de dados para si próprio ou para outra pessoa para quem a comunicação não seja destinada. Admite concurso ideal com outros crimes.	3
§ 202c – **Facilitação/Preparação de espionagem e interceção ilegítima de dados informáticos**	Prática de atos preparatórios para as infrações previstas nas § 202a e 202b; e.g. produzir, obter para si ou para outrem, vender, fornecer, divulgar ou tornar público, códigos de segurança que permitam o acesso ou programas informáticos cujo propósito é a prática de tais atos.	6
§ 202d – **Recolha ilegítima de dados informáticos**	Obter, fornecer, entregar, distribuir ou disponibilizar dados que não sejam geralmente acessíveis ou abertos ao público, e que tenham sido **obtidos por outra pessoa através de um ato ilícito**, a fim de se enriquecer a si próprio ou a outrem ou de prejudicar outra pessoa. Exceção: atos praticados exclusivamente no cumprimento de obrigações legais, e.g. autoridade pública no contexto de investigação.	
§ 303a – **Manipulação de dados informáticos**	Apagar, suprimir, inutilizar ou alterar dados informáticos.	4
§ 303b – **Sabotagem informática**	(1) Interromper significativamente uma operação de processamento de dados que seja de importância essencial para outra pessoa, através da prática dos atos descritos em § 303ª; ou através de introdução ou transmissão de dados com a intenção de infligir outra desvantagem; ou destruir, danificar, tornar inutilizável, remover ou alterar um sistema de processamento de dados ou um suporte de dados. (5) Aplica-se a § 202c, relativa à condenação de atos preparatórios ou facilitadores.	5

§ 269 – **Falsidade informática**	Com o intuito de provocar engano nas relações jurídicas, armazenar ou alterar dados relevantes em matéria de prova de tal forma que um documento falso ou falsificado seja produzido, ou que utilize dados armazenados ou alterados desta forma.	7
§ 270 – **Falsidade em tratamento informático de dados**	O engano nas relações jurídicas é equivalente à interferência num tratamento informático de dados nas relações jurídicas.	7

2. Aqueles cujo tipo corresponde a uma **ação cuja prática requer o uso e recurso a meios eletrónicos como instrumento** da prática do crime:

Quadro I-6: Condutas correspondentes a uma ação cuja prática requer o uso e recurso a meios eletrónicos como instrumentos

Artigo e epígrafe	Condutas	Artigo da CCCE
§ 206 – **Violação do sigilo postal ou de telecomunicações**	[1] Comunicar a outra pessoa, sem autorização, factos sujeitos ao segredo postal ou de telecomunicações e de que tenha tido conhecimento enquanto proprietário ou empregado de uma empresa que presta serviços postais ou de telecomunicações numa base comercial. [5] O sigilo do tráfego postal estende-se às circunstâncias pormenorizadas do envio e ao conteúdo. O **conteúdo das telecomunicações e as suas circunstâncias específicas** (quem esteve envolvido numa operação de telecomunicações), **estão sujeitos ao sigilo das telecomunicações**. O sigilo das telecomunicações também se estende às circunstâncias de **tentativas de ligação mal sucedidas**.	
§ 263a – **Burla informática**	[1] Com a intenção de obter uma vantagem patrimonial ilegítima para si próprio ou para terceiros, prejudicar a propriedade de outra pessoa, influenciando o resultado de uma operação de tratamento de dados através da conceção incorreta do programa, da utilização de dados incorretos ou incompletos, da utilização não autorizada de dados ou de qualquer outra influência não autorizada na operação. [3] Atos preparatórios como produção, aquisição, oferta para venda, manutenção em segurança ou entrega a outra pessoa de programas de computador cujo objetivo seja a prática de tal infração.	8
§ 265a – **Obtenção de serviços de modo fraudulento**	Utilizar máquina ou **rede de telecomunicações** que prosseguem interesses públicos, com o intuito de não pagar a taxa devida por transporte a meio de transporte, ou a acesso a um evento ou instalação.	

3. Aqueles cujo tipo corresponde a uma **ação que pode ser praticada** – mas não necessariamente – **através do recurso a meios eletrónicos** como instrumento da prática do crime.

Neste caso, importa notar a **§ 11 (3)** que prevê que meios como suportes de som e imagem, **suportes de armazenamento de dados**, ilustrações e outras representações são equiparados entre si,[73]

[73] Esta disposição está atualmente a ser revista e será adaptada aos novos desafios da cibercriminalidade. No Projeto de Lei do Governo de 4 de Setembro de 2019, a secção 11(3) diz o seguinte: "Os conteúdos na aceção das disposições referentes a este parágrafo são os contidos em escritos, em suportes de som ou imagem, em suportes de armazenamento de dados, ilustrações ou outras representações ou **são transmitidos independentemente do armazenamento através da tecnologia da informação ou da comunicação**". A lei ainda não foi adotada.

para os efeitos dos artigos que remetem para este número. Resulta assim que as seguintes incriminações preveem a prática por via de meios eletrónicos:

Quadro I-7:

Artigo e epígrafe	Condutas
§ 86 – **Divulgação de material de propaganda de organizações inconstitucionais**	Utilizar meios de propaganda – referidos em 11 (3) - que, de acordo com o seu conteúdo, se destinam a prosseguir os esforços contrários à ordem básica democrática livre ou aos princípios de direito internacional, sejam distribuídos no país ou produzidos, armazenados, importados ou exportados para distribuição no país ou no estrangeiro, ou tornado acessível ao público em dispositivos de armazenamento de dados.
§ 88 – **Sabotagem anticonstitucional**	(1) quem agir com intenção de perturbar ... (2) instalações de telecomunicações ao serviço público.
§ 91 – **Incitamento à comissão de ofensas graves e violentas contra o Estado**	Exibir ou fornecer a outrem materiais referidos em 11 (3) que, pelo seu conteúdo são aptos a servir como instrução para a prática de ofensas graves e violentas contra o Estado (§ 89a), se as circunstâncias da sua divulgação forem propícias à incitação ou estímulo à propensão de outros para o cometimento de tais ofensas, e/ou; (2) Obter materiais 11 (3) com o propósito descrito no (1) deste artigo.
§ 130 – **Incitamento ao ódio**	(2) Incitar ao ódio, apelar a medidas violentas ou atacar a dignidade humana de determinado grupo ou contra partes da população ou contra um indivíduo devido à sua pertença a um grupo, através dos meios referidos em 11 (3), para tal divulgando materiais ao público através de telecomunicações. (5) Publicamente aprovar, negar ou banalizar um ato de ódio cometido durante o domínio do nacional-socialismo e perturbar a paz pública de uma forma que viole a dignidade das vítimas ao aprovar, glorificar ou justificar as condutas do regime nacional-socialista de violência e de arbitrariedade, é igualmente punível se para o seu cometimento forem utilizadas telecomunicações.
§ 131 – **Representação de atos de violência**	(1) Através dos meios referidos em **11 (3)**, descrever atos de violência cruel ou desumana contra seres humanos ou que glorifique ou banalize tais atos, através de distribuição ao público ou produção, aquisição, fornecer, manter em stock, oferecer, anunciar ou comprometer-me a importar ou exportar esse tipo de conteúdo, para tal usando meios de radiofusão e telecomunicações.
§ 201a – **Violação da esfera íntima e privada pela captura de imagens**	(1) Produção ou transmissão/divulgação de gravação de imagem não autorizada de outra pessoa na sua esfera íntima e privada. (3) Tirar fotografias, produzir ou fornecer a terceiros em troca de benefício ou, obtenção para si mesmo ou para terceiros, de material relativo a nudez de menores de 18 anos.
§ 238 – **Perseguição**	Perturbar gravemente a vida de outra pessoa de modo a afetar seriamente o seu estilo de vida, através de, persistentemente: 1. Procurar proximidade física com essa pessoa, 2. Tentar estabelecer contacto com essa pessoa através de recurso a telecomunicações, 3. Utilização abusiva dos dados pessoais dessa pessoa a fim de a) efetuar encomendas de bens e serviços em seu nome, b) provocar o contacto com terceiros, ou 4. Ameaçar essa pessoa com danos à vida, à integridade física, à saúde ou à liberdade de si próprio, de um dos seus familiares ou de outra pessoa que lhe seja próxima.

Relativamente a crimes relacionados com menores, apesar de inseridos nesta última categoria (3), são aqui tratados separadamente:

Quadro I-8:

Artigo e epígrafe	Condutas	Artigo da CCCE
§ 176 – **Abuso sexual de crianças**	(1) Praticar atos sexuais com criança menor que 14 anos; (2) Induzir ou aliciar uma criança a praticar atos de natureza sexual; (4) Praticar atos sexuais na presença de criança ou apresentar a criança conteúdos pornográficos através de meios descritos em § 11(3) ou de **tecnologias da informação ou da comunicação**, a fim de levar a criança a praticar atos sexuais com o agente ou com terceiros, ou na presença destes, ou de levar a criança a praticar atos com vista à produção de conteúdo de pornografia infantil; (5) Oferecer ou prometer fornecer conteúdos relativos a crianças referentes aos atos descritos de (1) a (4).	9
§ 176a – **Abuso sexual de menores grave**	(3) Prática de atos descritos em § 176 como autor principal ou esteja de qualquer outra forma envolvido na prática dos atos, com a intenção de tornar o ato objeto de conteúdo pornográfico (§ 11 (3)) a ser divulgado nos termos do disposto no § 184b.	
§ 184b – **Divulgação e aquisição de pornografia infantil (menores de 14 anos)**	Divulgar, exibir ou de qualquer outro modo disponibilizar ao público conteúdos sexuais de menores, ou produzir, obter, fornecer, armazenar, oferecer, recomendar, importar ou exportar com aqueles fins, ou, de algum outro modo, facilitar/auxiliar o uso de meios descritos em § 11 (3) relativos a conteúdos sexuais de menores (inclui atos sexuais praticados com menores, atos praticados na presença de menores ou à representação de uma criança parcialmente ou integralmente nua em postura sexual explícita ou de representação da parte genital ou traseira da criança). (5) Exclui aplicação em casos de prosseguimento legal de funções públicas (e.g. no âmbito de ação penal).	
§ 184c – **Distribuição, aquisição e posse de literatura pornográfica juvenil**	Através dos meios descritos em § 11 (3), divulgar ou disponibilizar ao público, comprometer-se a entregar a outra pessoa, ou a produzir, obter, fornecer, armazenar, oferecer, publicitar ou a importar ou exportar um tipo de pornografia juvenil (entre 14 – 18 anos).	
§ 184d – **Divulgação de conteúdos pornográficos através de radiofusão ou telecomunicações**	(1) Colocar conteúdos pornográficos à disposição de outra pessoa ou do público **através da rádio ou telecomunicações** é punido nos termos do disposto nos §§ 184 a 184c (Não se aplica a casos descritos em § 184 (1) – divulgação de conteúdos pornográficos – desde que esses conteúdos digam respeito a maiores de 18 desde que não sejam acessíveis a menores de 18 anos); (2) Também se aplica aos §§ 184b (3) e 184c (3): será igualmente punido quem se comprometa a recuperar conteúdos pornográficos infantis através de meios eletrónicos.	

A tentativa é punível nos casos das secções 263a(2) conjugada com § 263(2), § 269(2), § 263a(3), § 303a, § 303b (vg. § 303a(2) e § 303b(3)). Relativamente a crimes relacionados com abuso de menores, a tentativa também é punível; § 176(6). Exceção: § 176(4)3 e 4 e § 176(5). Os atos preparatórios são puníveis nos crimes: § 202c, § 202a, § 202b, § 303a(1)(2) e § 303b (1)(5). A cumplicidade é também punível nos termos do disposto em § 26 e § 27 do StGB.

As pessoas coletivas não são sujeitos de responsabilidade criminal mas poderão ser responsabilizadas nos termos do disposto em §§ 30, 130 *Ordnungswidrigkeitengesetz* (OWiG) que diz respeito à Lei das infrações administrativas. Os seus representantes legais podem ser responsabilizados nos termos do disposto em § 14 do StGB.

Constata-se, deste modo, que cibercrime *lato sensu*, onde existe recurso às tecnologias de informação e comunicação para a prática do crime, estende-se a quase todas as infrações.

A lista que se segue não pretende ser exaustiva, limitando-se a mencionar outras proeminentes infrações que, apesar de não exclusivamente, podem ser cometidas através da internet:

- § 253 do Código Penal, chantagem;
- Violações dos direitos de autor ao abrigo da Lei Alemã de Direitos de Autor;
- § 284 do Código Penal, organização não autorizada de um jogo de azar;
- Tráfico de drogas ao abrigo da Lei Federal Alemã de Estupefacientes;
- Comércio de armas ao abrigo da Lei Alemã de Armas;
- Crimes de colarinho branco.

Para além das incriminações penais acima descritas, a legislação alemã prevê ainda outro tipo de ilícitos e contraordenações referentes a atos relacionados com comunicações eletrónicas e proteção de dados, sobre as quais será feito uma breve descrição.

A **Lei das Telecomunicações (TKG)**, aprovada em 06.22.2004, prevê um conjunto de obrigações para os prestadores de serviços de telecomunicações enquanto entidades privadas a observar na prossecução da sua atividade. Esta lei é, também, de particular importância relativamente à questão de preservação da prova digital, na medida em que prevê a obrigação de comunicação de atos que possam consubstanciar violações à inviolabilidade das telecomunicações e a obrigação de conservação de determinados dados para fins de procedimento criminal em caso de crimes especialmente graves.

Deste modo, os **§ 88 Confidencialidade das telecomunicações** e **§ 89 Proibição de interceção e obrigação de sigilo dos operadores das instalações recetoras** protegem a integridade e confidencialidade das telecomunicações e englobam o seu conteúdo e as suas circunstâncias pormenorizadas, e.g. quem está ou esteve envolvido num processo de telecomunicações, e estende-se também aos pormenores das tentativas infrutíferas de estabelecer uma ligação. É proibido às partes obrigadas obter o conhecimento destas telecomunicações para além do estritamente indispensável

para o exercício da sua atividade e a utilização destes conhecimentos para outros fins só é admissível na medida em que esta lei ou outra disposição legal o preveja. Neste caso, importante notar que o dever comunicação previsto na § 138 do Código Penal – obrigação de reportar crimes dos quais tenha conhecimento tem prioridade ao sigilo das comunicações.

O **§ 90** proíbe a **utilização abusiva de equipamentos de transmissão de telecomunicações** através da proibição de possuir, fabricar, distribuir, importar ou incluir qualquer emissor ou outro equipamento de telecomunicações que seja particularmente apto e se destine a ouvir a palavra não dita de outra pessoa ou a gravar a imagem de outra pessoa sem que esta a perceba.

Os **§§ 96 e 98** dizem respeito às condições em que os prestadores de serviço podem recolher **dados de tráfego e de localização**, respetivamente. Assim, só podem ser conservados os dados indispensáveis para os fins da sua atividade, e esses dados só podem ser utilizados na medida do necessário e para os fins mencionados nesta lei ou no cumprimento de outras disposições legais. Caso contrário, deverão ser apagados sem demora injustificada.

O **§ 109** obriga os prestadores de serviço à adoção de **medidas de proteção técnica** para proteger o sigilo das telecomunicações, e contra a violação da proteção de dados pessoais, tomando as precauções técnicas adequadas no tratamento de dados, de modo a protegê-los contra perturbações causadas por ataques externos. Assim, devem ser tomadas medidas para proteger os sistemas de telecomunicações e de processamento de dados contra o acesso não autorizado e para minimizar os efeitos das violações de segurança para os utilizadores ou para as redes interligadas. O (5) desta secção prevê ainda um dever de comunicação à Agência Federal de Redes e o Gabinete Federal para a Segurança da Informação de quaisquer deficiências nas redes e serviços de telecomunicações que possam conduzir a violações significativas da segurança. Igualmente, o **§ 109a** referente a **segurança de dados e da informação**, estabelece obrigações de comunicação em caso de violação de dados pessoais à Agência Federal de Redes e o Comissário Federal para a Proteção de Dados e Liberdade de Informação da violação e aos utilizadores visados.

Quanto à retenção de dados para efeitos de prova digital, o **§ 113b** estabelece a **obrigação de conservação de dados de tráfego** durante 10 semanas para dados de tráfego e durante 4 semanas para dados de localização. O conteúdo encontra-se excluído. O prestador de serviço apaga irreversivelmente os dados armazenados sem demora, mas o mais tardar no prazo de uma semana após o termo dos períodos de armazenamento previstos ou assegura o apagamento irreversível, v.g. Direito ao esquecimento.

O **§ 113c** estabelece **em que condições podem ser utilizados os dados armazenados** com base no § 113b; só podem ser transmitidos a uma autoridade de ação penal se esta última exigir essa transmissão, fizer referência a disposição legal que lhe permita recolher os referidos dados, e se tratar de repressão de infrações penais particularmente graves.

Como medida de segurança, o **§ 113d obriga os prestadores a garantir a segurança dos dados arma-**

zenados com base na obrigação prevista no § 113b (1). Assim, os dados devem ser protegidos contra o acesso e utilização não autorizados através de medidas técnicas e organizacionais em conformidade com o estado de evolução da tecnologia, através do uso de métodos de encriptação, entre outros.

A Agência Federal de Redes (*Federal Network Agency*) tem o poder de **monitorização do cumprimento de obrigações** previstas nesta lei para os prestadores de serviço (**§ 115**). Estes, por sua vez, estão obrigados a fornecer àquela as informações necessárias e a Agência tem poder de aplicar sanções pecuniárias compulsórias.

Lei de serviços de informação e comunicação eletrónicos (TMG), aprovada em 02.26.2007, é aplicável a todos os serviços de informação e comunicação eletrónicos, a menos que se trate de serviços de telecomunicações. De notar a obrigação prevista sobre os prestadores de serviços de informação e de página ou aplicação web ou para *smartphones* de assegurar, através de acordos adequados e economicamente proporcionais, que o acesso não autorizado não seja possível (**§ 13 (7)**). Por outro lado, existe também um **dever de prestar informação em caso de acesso ilegítimo a dados (§ 15a)**.

Lei de segurança informática (*IT-Sicherheitsgesetz*), aprovada a 25.07.2015, confere jurisdição ao departamento federal de procuradores para investigar e promover ação penal relativa aos crimes previstos em 202a, 202b, 202c, 263a, 303a e 303b do Código Penal.

Visa o reforço da segurança informática e em sistemas informáticos, e vem no decorrer da estratégia de cibersegurança aprovada em 2011. Para tal, estipula obrigações relativas a um nível mínimo de segurança informática para empresas de telecomunicações, fornecedores de serviços digitais e operadores de infraestruturas críticas, e.g. requer a implementação de um sistema de gestão de segurança informática, estipula obrigações de comunicação ao Departamento Federal de Segurança Informática (BSI) e a consumidores no caso de violação de sistema informático e obriga à recolha de informações necessárias para avaliação de riscos na segurança das tecnologias da informação, em modo de relatórios sobre ataques ocorridos, procedimentos adotados e riscos iminentes, a ser comunicado às autoridades federais (§ 4).

Neste momento, encontra-se para aprovação uma proposta de alteração desta lei, chamada *IT Security Act* (*IT-Sicherheitsgesetz*) 2.0.[74] A nova proposta funda-se numa mudança de estratégia no combate à cibercriminalidade que deverá deixar de ser defensiva para ser ofensiva, através do uso de diferentes táticas informáticas.[75] A proposta prevê também agravamento de penas previstas no código penal para os cibercrimes previstos em §§ 202a, 202b, 202c, 202d, 303a e 303b StGB. Ademais, §§ 202e e 202f são inseridos após § 202d StGB:

- § 200e – Utilização não autorizada do uso de sistemas de tecnologia de informação;
- § 202f – Ofensa particularmente grave contra o sigilo e integridade dos sistemas de tenologia e informação.

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

[75] 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/

A ***Netzwerkdurchsetzungsgesetz* (NetzDG)**, publicada a 01.09.2017, vulgarmente conhecida por Lei do Facebook, define obrigações e estabelece multas para os prestadores de redes sociais relativamente ao tratamento de queixas de utilizadores sobre crimes de ódio e outros conteúdos ilegais na Internet, bem como uma obrigação trimestral de comunicação por parte dos prestadores. Confere ainda direito a indemnização por violação de direitos personalidade e direito à informação sobre os dados do infrator registados nessa plataforma, ante ordem judicial.[76]

O §1 (3) define os conteúdos que são tidos como ilegais,[77] incluindo discriminação e incitamento ao discurso de ódio e discurso de extrema direita. O §2 define uma obrigação de comunicação periódica sobre o tratamento dado a queixas sobre conteúdos ilegais nas suas plataformas. Este relatório deve ser público. O *Federal Office of Justice* (BfJ) é a autoridade administrativa que monitoriza os relatórios, cf. a § 4 (4).

O § 3 (2) 2 prevê a **obrigação de remover ou bloquear o acesso ao conteúdo manifestamente ilícito no prazo de 24h** desde que recebe a queixa, exceto haja convenção em contrário com autoridades policiais ou judiciais. Demais conteúdo ilícito, deve ser removido ou bloqueado o acesso sem demoras, no prazo máximo de sete dias a contar da receção da queixa, cf. § 3 (2) 3. Em caso de remoção, o prestador é obrigado a preservar o conteúdo para efeitos de prova. Assim, armazena esses conteúdos durante um período de dez semanas no âmbito de aplicação das Diretivas 2000/31/CE e 2010/13/EU, cf. § 3 (3).[78]

O incumprimento destes deveres gera sanções administrativas.

Relativamente a obrigações processuais, as obrigações especiais previstas nos Artigos 16 e 17 da Convenção do Cibercrime não se encontram especificamente previstas no **Código de Processo Penal Alemão (StPO)**. Contudo, a apreensão de dados informáticos, incluindo pedidos de divulgação de dados, são efetuados ao abrigo da § 94 e § 98 StPO que regulamenta a apreensão geral de bens corpóreos.

O Artigo 18 da Convenção do Cibercrime, não se encontra, igualmente, previsto como tal no StPO. Nesse sentido, o pedido pelas autoridades de divulgação/informação relativa a dados informáticos encontra-se coberta pelo disposto na § 95 StPO, referente ao dever de entrega de objetos corpóreos relevantes para efeitos de prova em procedimento criminal.

A recolha de dados de tráfego de comunicações em tempo-real, prevista no Art. 20 da Convenção do Cibercrime, está sujeita aos requisitos da § 100g StPO. Este artigo também enuncia quais os crimes especialmente graves que justificam o fornecimento de dados por parte dos prestadores de serviços (cf. § 113b TKG). O § 100g (2) prevê ainda a possibilidade do tribunal ordenar a produção de dados de tráfego e informações aos prestadores de serviços no caso de fundadas suspeitas da prática de crime especialmente grave listado nesse artigo.

A interceção de telecomunicações ou recolha de dados em tempo real prevista no Art. 21 da

[76] Os prestadores de serviço de rede social que tenham menos de dois milhões de utilizadores registados na Alemanha estão fora do âmbito de aplicação da presente.

[77] A saber, artigos 86º, 86ºa, 89ºa, 91.º, 100ºa, 111º, 126º, 129.º, 129ºa 129ºb, 130º, 131º, 140º, 166º, 184ºb, em conjugação com os artigos 184º-D , 185º a 187º, 201º-A, 241º ou 269º do Código Penal.

[78] A Lei NetzDG encontra-se atualmente a ser revista e será alterada. O Parlamento e o Conselho alemães já aprovaram, mas a lei ainda não entrou em vigor. A nova lei incluirá a obrigação dos operadores dos meios de comunicação social de transmitirem os dados relevantes às forças policiais. Os objetivos são: reforçar os direitos dos utilizadores, tornar os canais de informação mais fáceis de utilizar, simplificar a execução de pedidos de informação e aumentar o valor informativo dos relatórios de transparência.

Convenção do Cibercrime é regulada pelas § 100a e 100b. Deve ser objeto de autorização judicial a requerimento do procurador. De modo geral, a recolha de dados através de pesquisa *online* e *spywares* não é admitida no âmbito de ação penal, exceto nos casos descritos em 100b.

§ 110 (3) – Possibilidade de acesso e inspeção de suportes de armazenamento separados espacialmente do principal que se encontrava sobre inspeção, na medida em que possam ser acedidos a partir do suporte de armazenamento. Exemplo: discos externos.

Pedidos de informação a/ou entrega de dados por parte dos prestadores de serviço às autoridades encontram-se regulados de modo geral na § 100j StPO e de particularmente nas leis avulsas; e.g. § 113 TKG.

As informações e dados serão prestados dentro dos limites previstos nas § 96 (1), § 113a e 113b TKG (Lei das telecomunicações).

No que concerne a **cooperação Internacional**, a Alemanha está envolvida em diversos projetos europeus e internacionais de cooperação bilateral na área da cibersegurança, nomeadamente:

- *European Network and Information Security Agency* (ENISA);
- Programa AGIS da Comissão Europeia, concebido para ajudar profissionais da área do direito, assim como autoridades judiciais e representantes de serviços de apoio às vítimas dos Estados Membros, e de outros países que se candidatem, com a vista a montar uma rede europeia para trocar informações e boas práticas;
- *Interpol European Working Party on IT Crime* (EWPITC), uma plataforma para troca de informações e combate aos crimes informáticos.

A **Lei de assistência legal internacional *(Internationale Rechtshilfe in Strafsachen - IRG)*** prevê procedimentos e condições para assistência internacional. Assim, os artigos 29-31 da Convenção do Cibercrime, referentes a assistência recíproca entre países, estão assegurados nessa lei.

Relativamente à cooperação com o Centro de Cibercrime da Europol, a Alemanha faz parte do *Joint Cybercrime Action Taskforce* (J-CAT).[79]

O ponto de contacto 24/7, de acordo com o previsto no Artigo 35 da Convenção de Budapeste, é estabelecido no BKA em *Wiesbaden*, juntamente com o ponto de contacto da Interpol e G-8.

Para mais, pode ainda verificar-se que existem algumas **parcerias público-privadas** dentro do território Alemão com vista ao **combate do cibercrime, nomeadamente**;

- Aliança para a Segurança Cibernética: promove a partilha de informações e experiências de entre os principais atores na arena da segurança cibernética alemã e visa atuar como uma plataforma de informação sobre os riscos preponderantes no ciberespaço e promover a par-

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

tilha de conhecimento. Uma iniciativa conjunta do Escritório Federal Alemão para Segurança da Informação (BSI) e da Associação Federal Alemã de Tecnologia da Informação (Bitkom);
- CERT Network - A rede CERT é a aliança de equipas de resposta de emergência a incidentes informáticos. [80]

Notas finais:

- A mera posse de *malware* não é incriminatória. A legislação nacional só incrimina estes factos quando uma pessoa os utiliza de modo a cometer um tipo criminal.
- Segundo alguns profissionais, é necessário introduzir disposições jurídicas no Código de Processo Penal para permitir a utilização de instrumentos de acesso a dados como *hacking*, tendo em conta que as forças de segurança consideram que estão um passo atrás dos infratores.
- De modo geral, a lei alemã parece estar em conformidade com os textos legais europeus.
- Todavia, não há uma transposição expressa dos artigos 4 e 5 da Diretiva 2019/713/EU, na medida em que é preciso recorrer a duas incriminações penais mais gerais (§§ 263a e 269 do Código Penal, respetivamente burla informática e falsidade informática) para cobrir infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento não em numerário. O § 152b do código penal prevê o crime de falsificação de cartões de pagamento, mas não faz qualquer referência ao recurso a meios eletrónicos ou através de sistemas informáticos.

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

3. PERSPETIVAS CRIMINOLÓGICAS E VITIMOLÓGICAS PARA A COMPREENSÃO DO CIBERCRIME

3.1. Teorias criminológicas aplicadas ao cibercrime

Neste capítulo do Manual, abordaremos, de forma sintética, diferentes teorias da criminalidade e a sua aplicação ao cibercrime, com o propósito de alcançar uma leitura tão compreensiva quanto possível do fenómeno da cibercriminalidade.

Na base de tal transposição, encontra-se a premissa de que o conhecimento existente acerca da criminalidade *tradicional* é também aplicável ao cibercrime, assumindo-se, portanto, que a criminalidade *tradicional* e a cibercriminalidade não são substancialmente distintas. Nesse sentido, as teorias criminológicas associadas ao crime *tradicional* assumem-se como ferramentas valiosas para explicar também o cibercrime (Wall, 2005, Yar, 2005b *cit in* Bossler & Burruss, 2012).

Todavia, importa salientar que não é possível uma compreensão plena do fenómeno criminal e do cibercrime em concreto, através da lente exclusiva de uma única teoria ou abordagem criminológica, sendo muito importante, atendendo inclusivamente à complexidade do fenómeno em análise, considerar o entrecruzamento destas (e de outras) perspetivas na procura de um entendimento mais robusto do cibercrime e da cibervitimação (Yar & Steinmetz, 2019).

3.1.1. Perspetivas individuais

Esta abordagem refere, *grosso modo*, que pessoas com níveis reduzidos de autocontrolo apresentam maior probabilidade de se envolverem em atos ilícitos (Gottredson & Hirschi, 1990 *cit in* Maimon & Louderback, 2019).

A esse respeito, Gottfredson e Hirschi (1990 *cit in* Higgins, Ricketts & Wolfe, 2014) argumentaram que as pessoas com **reduzido autocontrolo** se revelam menos capazes de resistir à tentação perante uma oportunidade ilícita, minimizando as consequências das suas ações, devido às características associadas a esse traço individual, nomeadamente a impulsividade e a insensibilidade (Gottfredson & Hirschi, 1990 *cit in idem*). Nesse sentido, o crime é atraente, uma vez que proporciona benefícios imediatos, sem serem considerados ou antecipados os impactos a longo prazo, tanto a nível individual, como para terceiros.

Da transposição desta abordagem explicativa da criminalidade *tradicional* para a compreensão do cibercrime, a associação entre as *características individuais do/a autor/a do cibercrime* e o *cibercrime* parece não ser tão linear, já que a investigação não se revela unânime quanto ao facto de os níveis reduzidos de autocontrolo representarem (ou não) um fator de risco individual para a prática de *cibercrimes* (Maimon & Louderback, 2019).

No caso do *cibercrime*, as características individuais podem não revelar-se tão significativas, uma vez que o cibercrime envolve uma menor (ou até inexistente) interação direta entre vítima e autor/a

do crime. Por exemplo, no caso de *malware*, é difícil determinar quem será a vítima em concreto da infeção pelo *software* malicioso, uma vez que qualquer computador pode ser potencialmente infetado, independentemente de características individuais dos/as intervenientes (Ngo & Paternoster, 2011).

Por outro lado, os níveis de autocontrolo parecem repercutir-se no risco de vitimação. Schreck, Stewart e Fisher (2006 *cit in* McNeeley, 2015) identificaram uma associação entre índices reduzidos de autocontrolo e menor propensão para evitar comportamentos de risco (como o envolvimento em atividades delinquentes e a socialização com pares desviantes), inclusivamente depois de experiências pessoais de vitimação. Essa ligação entre baixo autocontrolo e vitimação repetida foi confirmada por Turanovic e Pratt (2014 *cit in* McNeeley, 2015): pessoas com índices reduzidos de autocontrolo apresentaram menor probabilidade de efetuar alterações nos seus estilos de vida, mesmo após experiências de vitimação.

DESTAQUE | INFORMAÇÃO EM FOCO:

Algumas investigações em matéria de cibercrime, sobretudo de criminalidade ciber-dependente, têm identificado **fatores de risco individuais associados à perpetração**:

- Há estudos que referem que, no caso dos crimes ciber-dependentes, a maioria dos/as seus autores/as possui **competências técnicas relativamente reduzidas** (NCA, 2016 *cit in* Maimon & Louderback, 2019).
- Outros indicam, por outro lado, a associação do crime ciber-dependente a **caraterísticas psicológicas e cognitivas**, como a curiosidade, o pensamento criativo, a capacidade de resolução de problemas e de pensamento técnico sistemático (Rogers, 2006, Steinmetz, 2015 *cit in* Maimon & Louderback, 2019).

Outros autores (Morris, 2011 *cit in* Maimon & Louderback, 2019) apontam para o facto de o/a autor/a do cibercrime, nomeadamente no caso de crimes ciber-dependentes, desenvolver **atribuições causais claramente externas**, como técnicas de neutralização e racionalização, negando a existência da vítima, do cibercrime e/ou de responsabilidade no ato e/ou culpabilizando a vítima pelo facto de a prática do cibercrime ter sido possível.

No caso do *hacking*, van der Hulst e Neve (*cit in* Koops, 2010) distinguiram entre 3 tipos de *hackers*, associados a diferentes motivações:

- criminosos jovens rapazes, cuja prática do cibercrime se associa a diversão, curiosidade ou respeito pelos pares;
- *hackers* ideológicos, que são inteligentes e ansiosos por aprender, alguns dos quais obsessivos e com comportamentos antissociais;
- *hackers* financeiramente motivados.

3.1.2. Cibercrime enquanto escolha racional

Com uma abordagem que poderemos identificar como oposta à anterior, no seio da criminologia neoclássica, a criminalidade emerge enquanto resultado de processos cognitivos racionais de reflexão e decisão a cargo dos/as respetivos autores/as. Quer isto dizer que o crime corresponde a uma **decisão racional por parte do/a seu/a agente**, que analisa os custos e os benefícios associados à sua prática, e cujas escolhas/decisões são orientadas por esses mesmos processos de análise e reflexão (Cornish & Clarke, 1986 *cit in* Yar & Steinmetz, 2019).

No seguimento dessa abordagem, caso o/a eventual autor/a de um crime percecione os custos associados à sua prática, que podem incluir a probabilidade/risco de deteção e as consequências legais associadas, como reduzidos, comparativamente aos ganhos ou benefícios eventualmente obtidos no caso de tal crime ser cometido, a probabilidade de ocorrência do crime aumenta (Nagin, 1998 *cit in idem*).

Tendo por base esta interpretação, o incremento dos **custos percecionados associados à prática de um crime** e/ou a redução da perceção dos **benefícios, ganhos e/ou recompensas com a sua realização** poderão contribuir para a mitigação do crime (Cornish & Clarke, 1986 *cit in idem*).

Estudos como os de Louderback & Antonaccio (2017) apontam para o facto de processos cognitivos reflexivos poderem reduzir ou aumentar o risco de envolvimento na criminalidade ciber-dependente. Na base deste racional encontra-se precisamente o facto de se entender o **cibercrime enquanto escolha**, na qual é realizada uma avaliação racional dos esforços, custos e recompensas associadas a um determinado comportamento (Cornish, 1993 *cit in* Maia et al., 2016).

Algumas investigações associadas à aplicação desta abordagem na explicação de crimes ciber-dependentes (e.g., Bachmann, 2008, Hutchings, 2013 *cit in* Yar & Steinmetz, 2019) apontam para o facto de o/a autor/a do cibercrime realizar efetivamente escolhas racionais na seleção dos seus alvos e também na adoção de comportamentos de risco.

A escolha racional parece também ter lugar, inclusivamente perante alvos em que existe intencionalmente, com propósitos dissuasores da prática do cibercrime, indicações claras da existência de consequências associadas à prática de cibercrime, existindo modificação do comportamento criminal (mas não necessariamente a dissuasão face à efetivação do cibercrime) (e.g., Maimon et al., 2013 *cit in idem*).

3.1.3. Teoria do estilo de vida

Já a **teoria da exposição ao estilo de vida** de Hindelang, Gottfredson e Garofalo (1978 cit in Phillips, 2015) afirma, resumidamente, que o estilo de vida quotidiano de uma determinada pessoa influencia a quantidade de exposição a locais e horários em que existe maior risco de ocorrência de crime.

Nesse sentido, as diferenças nas taxas de vitimação em diferentes grupos demográficos devem-se precisamente às variações no estilo de vida, no qual se incluem as atividades diárias rotineiras, as atividades vocacionais (incluindo ocupação profissional e escolar/académica) e as atividades de lazer (Hindelang et al., 1978, p. 241 *cit in* McNeeley, 2015), que poderão aumentar ou diminuir a exposição a lugares e pessoas de alto risco nos momentos em que é mais provável a ocorrência de crimes.

A mesma teoria postula que características demográficas, como idade, sexo, estado civil, estatuto socioeconómico, educação e ocupação, afetam os estilos de vida, uma vez que resultam em implicações para os papéis, comportamentos, atividades e atributos socialmente construídos que uma determinada sociedade considera serem adequados para uma pessoa com determinadas características.

Identicamente, o **estilo de vida de uma determinada pessoa na Internet**, no qual se incluem as atividades sociais, como conversar, publicar e/ou partilhar conteúdo em qualquer rede social, as atividades profissionais, como comunicar por *e-mail*, realizar áudio/videochamadas e/ou partilhar e armazenar ficheiros em serviços/aplicações de armazenamento e sincronização, bem como atividades rotineiras, como comprar produtos, efetuar pagamentos, consultar *websites* e usar aplicações, pode ser visto como um determinante da exposição ao cibercrime (van Wilsem, 2011).

Igualmente, o estilo de vida de uma pessoa influencia também o seu risco de envolvimento em atividades ilícitas, oferecendo a oportunidade para o envolvimento em comportamentos criminosos (talvez com pares desviantes) e afastando-a da supervisão de pares normativos e outros relacionamentos protetores (McNeeley, 2015).

Essa teoria foi combinada com a teoria das atividades de rotina, descrita abaixo, para uma explicação mais geral dos eventos de crime/vitimação (*idem*).

3.1.4. Teoria das atividades de rotina

No seguimento da teoria do estilo de vida, a teoria das atividades de rotina procura explicar a ocorrência do crime, através da conjugação das seguintes condições:

- criminoso/a motivado/a;
- alvo/vítima adequado;
- ausência de vigilância (Cohen & Felson, 1979 *cit in* Maimon & Louderback, 2019).

Se uma (ou mais) destas três condições estiverem ausentes, a probabilidade de ocorrência de crime diminui (Phillips, 2015).

No que respeita ao/à **cibercriminoso/a**, a proximidade da vítima relativamente a cibercriminosos/as motivados aumenta o risco de vitimação (van Wilsem, 2013 *cit in* Maimon & Louderback, 2019).

DESTAQUE | INFORMAÇÃO EM FOCO:

A motivação para a prática de um cibercrime poderá ser **situacional**, nomeadamente pela presença de um estímulo que, independentemente de qualquer característica pessoal, possa levar ao envolvimento na prática de cibercriminalidade (Briar & Piliavin, 1965 *cit in* Maimon & Louderback, 2019). Estes estímulos podem associar-se à ocorrência do denominado **crime motivado pela oportunidade** o que, no caso da criminalidade ciber-dependente, poderá referir-se a vulnerabilidades num determinado sistema operativo, à ausência de sistemas de segurança e/ou à disponibilização de dados não encriptados. Estas circunstâncias reduzem o risco de deteção para o/a cibercriminoso/a, o que, por sua vez, aumenta a probabilidade de ocorrência de crimes ciber-dependentes (Willison & Siponen, 2009 *cit in* Maimon & Louderback, 2019).

A **adequabilidade** do alvo/vítima é avaliada racionalmente pelo potencial autor/a do crime, através do valor ou desejabilidade do alvo, da sua visibilidade, inércia e acessibilidade (Felson, 2002 *cit in* Maia et al., 2016).

Ainda relativamente à adequabilidade do alvo, no caso da cibercriminalidade, atendendo à acessibilidade e à dimensão de utilizadores/as da (e na) Internet, poderá considerar-se que as oportunidades para a prática de cibercrime são maiores do que a prática de crimes no mundo físico (Saridakis, Benson, Ezingeard & Tennakoon, 2016).

Os níveis de utilização das TIC e da Internet parecem constituir um importante indicador relativo à **adequabilidade do alvo**, isto é, as pessoas com períodos mais prolongados de utilização das TIC apresentam maior risco de cibervitimação. O estudo de Wang e colegas (2015 *cit in* Maimon & Louderback, 2019) veio demonstrar que, de facto, a acessibilidade, a visibilidade e a exposição do alvo podem aumentar o risco de cibervitimação. Ainda no âmbito da **adequabilidade**, a cibercriminalidade é também mais frequente em países mais ricos e, como tal, com mais utilizadores/as da (e na) Internet (Kigerl, 2012 *cit in* Maimon & Louderback, 2019).

Já no que respeita à cibercriminalidade dirigida a empresas e organizações, a adequabilidade do alvo aumenta o risco de cibervitimação. Nesse sentido, o cibercrime é mais frequente ao longo do horário de funcionamento das respetivas empresas ou organizações, durante o qual o número de alvos disponíveis é maior (Kigerl, 2012 *cit in* Maimon & Louderback, 2019).

Por seu turno, a **vigilância**, no caso da cibercriminalidade e, em concreto, dos crimes ciber-dependentes, envolve (Grabosky, 2016 cit in Maimon & Louderback, 2019):

- Autoridades policiais;
- Organizações governamentais responsáveis pela gestão e monitorização do ciberespaço;
- ISP (*Internet Service Providers*), empresas e indústrias que recorrem a diferentes ferramentas e práticas de prevenção do cibercrime.

Ao nível da cibercriminalidade, a vigilância poderá ser analisada a partir de diferentes dimensões (Bossler & Holt, 2009, Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019). Assim:

- a ausência de **vigilância social** (ex.: supervisão parental aquando da utilização da Internet por parte de crianças) parece estar associada a um aumento de probabilidade de ocorrência de crimes ciber-dependentes;
- ainda que não seja unânime, a **vigilância física** (na qual se inclui a utilização de sistemas ou *softwares* de segurança nas TIC) está associada à redução do risco de cibervitimação;
- a presença de **vigilância pessoal** (que diz respeito a conhecimentos e competências de utilização das TIC e da Internet) reduz a cibervitimação por crimes ciber-dependentes.

Por fim, e de forma integrada, a teoria do estilo de vida e das atividades de rotina enfatizam a ideia de que as **atividades e comportamentos rotineiros do estilo de vida de uma determinada pessoa poderão aumentar os seus níveis de adequabilidade enquanto (potencial) alvo de cibercrime** e a sua exposição a potenciais cibercriminosos/as, o que, na ausência de mecanismos de vigilância, aumenta o risco de vitimação e de cibervitimação (Cohen, Kluegel & Land, 1981 *cit in* Phillips, 2015).

3.1.5. Outras abordagens relevantes

De forma sintética, a **teoria da aprendizagem social** aponta o crime enquanto comportamento aprendido, como qualquer outro comportamento.

Esse processo de aprendizagem envolve:

- interações de um indivíduo com outros num determinado grupo;
- atitudes de um indivíduo em relação a um comportamento, incluindo técnicas, racionalização e motivação para executar um comportamento;
- imitação, incluindo visualização e repetição de um determinado comportamento de outros elementos do grupo;
- reforço, incluindo recompensas que promovem o início e a manutenção de um comportamento.

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

A teoria da aprendizagem social parece igualmente consistente para a explicação da cibercriminalidade: atendendo ao facto de entender que o comportamento criminal é aprendido, através de um processo de imitação de pares e assimilado por mecanismos de reforço positivo, a **associação com pares semelhantes** parece relacionar-se com o envolvimento na prática de cibercrimes (Hutchings & Clayton, 2016 *cit in* Maimon & Louderback, 2019).

Progredindo-se, deste modo, de abordagens ou perspetivas individuais, associadas às características

psicológicas, emocionais e processos cognitivos de um determinado indivíduo, para as suas relações interpessoais, importa destacar o **envolvimento em redes mais ou menos organizadas de pares da *deep web***, com uma **subcultura e estrutura (hierárquica)** própria, enquanto fator de risco para a perpetração de cibercrimes (Macdonald & Frank, 2017 *cit in idem*). Diga-se aliás, que as **relações de lealdade** são apontadas em alguns estudos como motivações para o envolvimento em práticas de cibercriminalidade, nomeadamente no caso de crimes ciber-dependentes (Hutchings & Clayton, 2016 *cit in idem*).

A incursão pela cibercriminalidade pode também ser explicada à luz de três dimensões (Thornberry, Krohn, Lizotte & Chard-Wierschem, 1993 *cit in* Peterson & Densley, 2017):

- a **seleção**, segundo a qual a causa da cibercriminalidade não assenta na Internet em si, mas antes nos fatores de risco individuais e de propensão criminal presentes nas pessoas que utilizam a Internet, as TIC e as redes sociais;
- a **facilitação**, segundo a qual a Internet e as TIC têm efeito na facilitação da cibercriminalidade, considerando algumas das características propícias do contexto *online*, como o anonimato, a falta/ausência de supervisão e os processos de grupo (como a conformidade com as normas do grupo, por exemplo);
- a **melhoria ou aperfeiçoamento**, que combina os conceitos anteriormente elencados – seleção e facilitação –, explicando que a ocorrência de cibercriminalidade se associa à **presença de fatores de risco individuais nas pessoas mais propensas à prática de cibercrimes** e às já referidas **características da Internet**, das redes sociais e das TIC que potenciam a expressão da propensão criminal.

3.2. A vítima de cibercrime e os fatores de risco associados à cibervitimação

Como já abordado no ponto 1 deste Manual, o "ecossistema" da cibercriminalidade e das suas diferentes formas de expressão inclui um interveniente ou figura frequentemente secundarizada ou negligenciada na compreensão do fenómeno criminal: referimo-nos, em concreto, às **vítimas de crime**.

DESTAQUE | INFORMAÇÃO EM FOCO:

De acordo com a Diretiva 2012/29/UE do Parlamento Europeu e do Conselho de 25 de outubro de 2012 que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade[81], a definição de *vítima* considera:

i. *uma pessoa singular que tenha sofrido um dano, nomeadamente um dano físico, moral ou emocional, ou um prejuízo material diretamente causados por um crime,*
ii. *os familiares de uma pessoa cuja morte tenha sido diretamente causada por um crime e que tenham sofrido um dano em consequência da morte dessa pessoa.*

[81] Documento completo está disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX-%3A32012L0029.

3. PERSPETIVAS CRIMINOLÓGICAS E VITIMOLÓGICAS PARA A COMPREENSÃO DO CIBERCRIME

Por outras palavras, a **vítima de crime** é uma pessoa que, em consequência de ato praticado contra as leis penais em vigor, sofreu um ataque contra a sua vida, integridade física ou mental, um sofrimento de ordem emocional ou uma perda material. Consideram-se também vítimas os/as familiares próximos ou as pessoas a cargo da vítima direta, bem como as pessoas que tenham sofrido algum tipo de dano ao intervirem para prestar assistência às vítimas ou para impedir a vitimação.

Segundo o *IVOR Report: Implementing Victim-Oriented Reform of the criminal justice system in the European Union*,[82] relatório que reflete sobre a investigação, o conhecimento científico e empírico relativamente à implementação prática dos direitos das vítimas de crime na Europa, a existência de uma definição clara, pelo menos do ponto de vista legal, do conceito de *vítima de crime* contribui não apenas para o melhor apoio e proteção às vítimas, como também promove uma maior **consciencialização e reconhecimento da figura da vítima** no fenómeno criminal e no sistema de justiça.

Neste ponto do Manual, procuraremos, precisamente, dar visibilidade às vítimas que, em consequência de um (ou mais) crimes ciber-dependentes e/ou de qualquer crime possibilitado ou facilitado pela Internet e pelas TIC, tenham sofrido qualquer dano, seja ele físico, moral, mental, emocional ou material. Começaremos, para o efeito, por abordar alguns dos fatores de risco associados à cibervitimação.

Os **fatores de risco**[83] dizem respeito a características, condições ou variáveis associadas a uma determinada pessoa que aumentam a probabilidade de ocorrência de resultados negativos ou indesejáveis (Reppold et al., 2002 *cit in* Maia et al., 2016).

Podem ser estáticos ou dinâmicos, sendo que os estáticos dizem respeito a características ou condições da pessoa e/ou do seu passado que não são passíveis de modificação, tais como, por exemplo, o sexo, as experiências pessoais de violência na infância ou a perda de um familiar. Por outro lado, os fatores de risco dinâmicos referem-se a características, condições ou variáveis modificáveis que aumentam a probabilidade de ocorrência de um determinado problema.

Deste modo, concetualizando a cibercriminalidade como um problema ou resultado negativo, **os fatores de risco** associados à cibervitimação são características ou condições que podem aumentar a probabilidade ou a vulnerabilidade de uma determinada pessoa face ao cibercrime.

A investigação não é particularmente extensa neste domínio, como em muitos outros associados à compreensão do cibercrime. Ainda assim, destacam-se os seguidamente apresentados.

3.2.1. Fatores de risco associados às características sociodemográficas

A associação entre **sexo** e risco de cibervitimação não é, de todo, linear, sendo importante atender

[82] Informação adicional sobre a reflexão em torno da definição do conceito de vítima de crime e outras matérias relativas aos seus direitos e sua implementação efetiva está disponível no relatório completo, em https://apav.pt/publiproj/images/yootheme/PDF/IVOR-Repot-WebVersion.pdf.

[83] Não sendo o propósito do presente conteúdo, importa, todavia, esclarecer que o conceito de fator de risco não poderá dissociar-se do conceito de fator de proteção que, sinteticamente, diz respeito a características ou condições que podem diminuir a probabilidade de aparecimento ou ocorrência de um determinado problema.

também, pelo menos, aos diferentes tipos de cibercrime, sob pena de uma leitura redutora da vulnerabilidade ao cibercrime. Veja-se os dados seguintes.

Muito embora sem consenso, alguns estudos apontam para o facto de o sexo feminino apresentar maior probabilidade de ser vítima de crimes ciber-dependentes (Bossler & Holt, 2009, 2010, Ngo & Paternoster, 2011 *cit in* Maimon & Louderback, 2019). O mesmo parece decorrer no caso do *ciber-stalking* (Holt & Bossler, 2008), com índices superiores de prevalência a afetar o sexo feminino, assim como no *ciber-bullying*.

Por outro lado, no caso das situações de abuso e exploração sexual de crianças *online*, apesar de a proporção de vítimas do sexo feminino se superiorizar face à dimensão de situações de abuso e exploração sexual *online* contra crianças do sexo masculino, pelo menos no que respeita aos casos identificados, estes últimos são, por norma, alvo de formas mais graves, severas e intrusivas de agressão sexual[84].

Já no que respeita à exposição (nomeadamente de crianças e jovens), por exemplo, a conteúdos de discursos de ódio *online*, as diferenças na média europeia de índices de exposição entre meninas/raparigas e meninos/rapazes são mínimas. O mesmo cenário foi identificado na receção de conteúdos auto produzidos de natureza sexual/*sexting*, com médias muito semelhantes em ambos os sexos[85].

Igualmente, também a **idade** apresenta, nos estudos e investigações realizados até à data, uma relação inconsistente com o risco de cibervitimação (Bossler & Holt, 2009, Ngo & Paternoster, 2011 *cit in* Maimon & Louderback, 2019). No entanto, há estudos que indicam que as pessoas mais velhas são, com maior frequência do que outras pessoas adultas, vítimas de cibercrime, nomeadamente de crimes ciber-dependentes, como o *hacking* (Leukfeldt & Yar, 2016 *cit in* Maimon & Louderback, 2019).

Por outro lado, e em termos genéricos, a população mais jovem, como abordaremos em seguida, apresenta índices elevados de utilização intensiva das TIC e da Internet, concretamente das redes sociais, o que resultará numa maior vulnerabilidade à cibervitimação, em comparação com utilizadores/as mais velhos e com utilizadores/as menos frequentes (Staksrud, ÓLafsson & Livingstone, 2013 *cit in* Näsi, Oksanen, Keipi & Räsänen, 2015; Näsi et al., 2015).

Já no que respeita à **escolarização**, há estudos que apontam para a possível existência de uma relação negativa entre o nível de escolarização e a cibervitimação, nomeadamente por crimes ciber-dependentes, por *hacking*, ou seja, níveis mais elevados de escolarização estarão associados a um menor risco de cibervitimação (van Wilsem, 2013 *cit in* Maimon & Louderback, 2019). Todavia, como nas características sociodemográficas anteriores, o efeito deste fator de risco carecerá de investigação adicional, atendendo à insipiência do conhecimento em matéria de risco de cibervitimação associado a características individuais.

[84] Informação adicional e detalhada esta disponível em https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database.

[85] Veja-se, para o efeito, os resultados do inquérito *EU Kids Online 2020: Survey results from 19 countries*, já citado em outros pontos deste Manual, disponível para consulta em https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf.

3.2.2. Fatores de risco associados à utilização da Internet e das TIC

O conceito de **literacia tecnológica** diz respeito à consciência, conhecimento e competências que permitem a uma determinada pessoa a utilização eficaz da Internet, das TIC e dos equipamentos e ferramentas associadas e a movimentação em ambientes digitais (Holt & Bossler, 2013 *cit in* Maimon & Louderback, 2019).

Constitui, por isso mesmo, um importante fator na determinação dos níveis de risco e de proteção face à cibervitimação. As competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação, também pelo facto de garantirem ao/à utilizador/a uma maior capacidade para identificar e atuar perante situações em que a sua segurança *online* possa estar em risco (Holt & Bossler, 2008).

São vários os estudos que apontam para a existência de um aumento da vulnerabilidade à cibervitimação por diferentes formas de cibercrime, como seja o *hacking*, o *malware* e o *phishing*, em função dos **níveis de utilização da Internet e das TIC** (Yucedal, 2010; Leukfeldt & Yar, 2016; Reyens, 2015 *cit in* Maimon & Louderback, 2019). Parece, por isso, existir uma associação entre o nível de atividade nas TIC e a vitimação por cibercrime: pessoas com mais hábitos de utilização das redes sociais e das TIC em geral nas suas atividades diárias apresentam também níveis mais elevados de experiências pessoais de vitimação por cibercrime (Butler, 2013). Esta constatação alinha-se, desde logo, com as teorias criminológicas já abordadas neste Manual.

DESTAQUE | INFORMAÇÃO EM FOCO:

O risco aumentado de cibervitimação em função dos níveis de utilização das TIC não deverá, contudo, ser interpretado de forma linear em que, per se, a utilização das TIC e da Internet aumenta o risco de cibervitimação.

São sobretudo os **comportamentos e o tipo de atividades encetadas aquando da utilização das TIC e da Internet** os principais fatores que contribuem para a maior vulnerabilidade à vitimação por cibercrime (Butler, 2013; Holt & Bossler, 2008).

Esta vulnerabilidade será abordada, em maior detalhe, no tópico seguinte deste Manual.

3.2.3. A vulnerabilidade comportamental e a sua associação à cibervitimação

DESTAQUE | ESTATÍSTICAS EM FOCO:

De acordo com os dados do já citado estudo transnacional *Health Behaviour in School-aged Children*, 35% dos/as adolescentes inquiridos/as consideram-se **utilizadores/as muito intensivos da Internet e das TIC**, isto é, utilizam estas ferramentas diariamente e durante uma parte significativa dos seus dias.

Adicionalmente, 1 em cada 10 adolescentes aponta a utilização intensiva da Internet e das TIC para comunicar com pessoas que conheceu apenas através da Internet.

Em média cerca de 7% dos/as adolescentes revelam ainda **comportamentos de adição** associados à utilização da Internet e das TIC, com destaque para o sexo feminino.

Em linha com o que já foi referido na teoria do estilo de vida e na teoria das atividades de rotina (veja-se ponto 3.1. deste Manual), o estilo de vida *online* de uma pessoa afeta o risco de cibervitimação a que pode estar exposta (Yucedal, 2010).

Neste estilo de vida *online* inclui-se todo o **tipo de atividades realizadas na Internet ou através da Internet e das TIC**, seja no que respeita às interações sociais e atividades mais lúdicas, bem como ações e tarefas associadas à ocupação profissional, escolar ou outra e inclusivamente tarefas rotineiras, como as próprias abordagens teóricas da criminologia referem, nas quais se inserem as compras *online*, a realização de pagamentos e mesmo o agendamento de compromissos e/ou o cumprimento de obrigações face ao Estado. Integra-se, igualmente, a frequência e intensidade de utilização da Internet e das TIC.

Ao abrigo deste conceito - estilo de vida *online* - claramente abrangente, torna-se claro que os níveis de risco de cibervitimação não são iguais para qualquer atividade realizada na Internet ou através da Internet e das TIC e para diferentes hábitos de utilização.

Algumas atividades, como o *download* de programas de *freeware*[86] ou a utilização de *websites* de compartilhamento de arquivos, apresentam um nível maior de risco de cibervitimação do que outras atividades, como verificar *e-mails* ou visitar canais de notícias *online*. Similarmente, as pessoas que se envolvem em atividades *online* menos seguras, como visitar *websites* desconhecidos e/ou efetuar *download* de músicas, vídeos, filmes e/ou jogos em plataformas não oficiais, apresentam maior probabilidade de serem alvo de alguma forma de cibervitimação (Choi, 2008, Moitra, 2005, Yar, 2005, 2006 *cit in* Yucedal, 2010). Por sua vez, a utilização da *webcam*, a realização frequente de compras *online* e a aceitação de pedidos de amizade nas redes sociais provenientes de pessoas/perfis desconhecidos aumen-

[86] *Freeware* diz respeito a *software* ou programas de computador cuja utilização não requer a aquisição de licença/pagamento monetário.

tam o risco de cibervitimação, comparativamente ao risco de cibervitimação evidenciado por pessoas sem tais hábitos de utilização da Internet e das TIC (Clarke, 2004; van Wilsem, 2011; Butler, 2013).

DESTAQUE | INFORMAÇÃO EM FOCO:

No que diz respeito ao estilo de vida *online* e aos comportamentos de utilização da Internet, importa ainda referir que as **pessoas com experiências pessoais de perpetração ou de envolvimento no cibercrime apresentam também maior risco de experienciação de cibervitimação** (Choi, 2008, Wolfe et al., 2008, Bossler & Holt, 2009, van Wilsem, 2013 *cit in* Maimon & Louderback, 2019).

Este risco aumentado de vitimação por parte de pessoas envolvidas em atividades ilícitas é identicamente encontrado na criminalidade *tradicional*, estando associado ao estilo de vida, aos seus comportamentos e a níveis diferenciados de exposição a circunstâncias, contextos e pessoas/grupos de risco (veja-se síntese das teorias criminológicas no ponto 3.1. deste Manual).

Nesta matéria, e no caso da cibercriminalidade, o já referido envolvimento e pertença a subculturas criminais específicas associam-se ao risco de perpetração de cibercrime (Macdonald & Frank, 2017 *cit in* Maimon & Louderback, 2019), mas também ao de cibervitimação, pela exposição a pares também desviantes.

Para um melhor entendimento da relevância dos comportamentos na utilização da Internet e das TIC e da sua associação com a vulnerabilidade à cibervitimação, torna-se premente abordar o **efeito de desinibição**, uma característica marcante associada à utilização da Internet e das TIC. Entenda-se, para o devido enquadramento, que este processo ou efeito de desinibição resulta do modo como a distância física a que a interação ou comunicação ocorre, a ausência de contacto direto no processo de comunicação, o maior anonimato e a perceção de maior controlo sobre o processo de interação parecem contribuir para uma maior facilidade na partilha de informação, na expressão livre de emoções e pensamentos e na adoção de comportamentos que não seriam, respetivamente, partilhados, expressos e praticados no caso de as interações terem lugar em contextos convencionais (Suler, 2004; Martellozzo & Jane, 2017). Este efeito de desinibição, aparentemente vantajoso, poderá contribuir para a exposição a situações e/ou para a adoção de comportamentos *online* que aumentam a vulnerabilidade à cibervitimação (Agustina, 2015).

DESTAQUE | PRÁTICAS EM FOCO:

No já longínquo ano de 1995, um grupo de trabalho de uma empresa sediada nos Estados Unidos da América desenvolveu um memorando denominado *Netiquette Guidelines*, no qual terá sido, pela primeira vez, utilizado o conceito de ***netiquette***, traduzível como um conjunto de regras de comportamento, incluindo regras de comunicação e normas de segurança, aplicáveis a pessoas e entidades coletivas, tendo em vista uma utilização segura e adequada da Internet e das suas diferentes ferramentas de comunicação.

O documento original está disponível em https://www.ietf.org/rfc/rfc1855.txt.

Nesse sentido, salienta-se a importância da **consciencialização**, do **conhecimento** e das **competências** de **controlo face ao tipo e à dimensão de informação pessoal partilhada ou partilhável** na Internet e, em concreto, nas redes sociais. A esse respeito, foi identificada uma associação significativa entre a perceção de risco de/para a privacidade, o controlo percebido face à informação partilhável e os comportamentos de partilha de informação nas redes sociais: as pessoas com níveis mais elevados de controlo percebido face à informação partilhada/partilhável, compartilham de forma mais criteriosa, percecionam-se como mais seguras e apresentam menor probabilidade de serem vítimas de cibercrime (Hajli & Lin, 2014 *cit in* Saridakis et al., 2016).

3.3. As entidades coletivas enquanto alvos do cibercrime

O cibercrime tem também o potencial de afetar entidades coletivas, transpondo as barreiras da vitimação individual sobre a qual nos temos debruçado ao longo deste Manual.

Referimo-nos, em concreto, às situações em que os alvos do cibercrime são **empresas, multinacionais, instituições e mesmo infraestruturas governamentais** (Yucedal, 2010; Näsi et al., 2015).

Estas entidades podem sofrer perdas substanciais na sequência da cibercriminalidade de que possam ser alvo, seja na forma de clientes perdidos e/ou de informações confidenciais comprometidas ou furtadas, seja através de perdas financeiras imediatas, que podem inclusivamente afetar e lesar os/as clientes, a nível individual, assim como perdas futuras, associadas à diminuição na confiança dos/as clientes nos produtos e/ou serviços que providenciam (Nykodym, Taylor & Vilela, 2005, 2005; Kratchman et al., 2008).

DESTAQUE | INFORMAÇÃO EM FOCO:

A componente humana representa também, na cibercriminalidade praticada contra entidades coletivas, um papel de relevo. Referimo-nos ao **papel de profissionais e trabalhadores/as** dessas mesmas entidades e aos seus **níveis de implementação das políticas e medidas organizacionais de segurança** contra o cibercrime, assim como aos seus comportamentos pessoais de cibersegurança.

Sabe-se que a apreciação adequada das vulnerabilidades organizacionais por parte de profissionais e trabalhadores/as produz efeito positivo nos níveis de cumprimento de estratégias e políticas de segurança adotadas por uma determinada empresa ou organização (Johnston & Warkentin, 2010 *cit in* Maimon & Louderback, 2019; Siponen et al., 2010 *cit in* Maimon & Louderback, 2019).

O ciberterrorismo, sumariamente apresentado no ponto 1 deste Manual, é exemplo deste cibercrime que visa entidades coletivas, uma vez que a sua intenção, como também já foi indicado, se centra na

destruição e/ou incapacitação de infraestruturas críticas para o funcionamento de uma sociedade ou de um Estado, e não necessariamente no dano a cidadãos/ãs individuais (o que não quer dizer que tal não venha também a ocorrer na sequência da sua efetivação).

Também neste âmbito, emerge o conceito de *hacktivism*, que resulta de uma interseção entre o ativismo político e as TIC, através das quais o *hacking* assume propósitos ou causas políticas (Yar & Steinmetz, 2019).

DESTAQUE | INFORMAÇÃO EM FOCO:

O movimento internacional descentralizado de *hacktivism* Anonymous, surgido na Internet na década de 2000 e conhecido pela prática de *hacking* e *DDoS* (veja-se ponto 1.3. deste Manual, para mais informações sobre estas formas de cibercrime), tem sido associado a diversos ataques contra infraestruturas governamentais, multinacionais, instituições financeiras e entidades religiosas.

Os objetivos deste movimento não são claros, mas associar-se-ão, de acordo com os próprios, ao combate à censura e opressão e à promoção da liberdade de expressão.

4. OS CUSTOS E O IMPACTO DO CIBERCRIME

Neste ponto do Manual, procuraremos percorrer um conjunto de sintomas e indicadores de impacto da cibervitimação, sendo certo que, atendendo à multiplicidade e vasto escopo de fenómenos em análise, as consequências seguidamente apresentadas serão sempre redutoras e genéricas, não contemplando a individualidade de cada experiência particular e pessoal de cibervitimação.

Procuraremos, igualmente, abordar os custos financeiros e económicos associados ao cibercrime, assumindo-se que, muito embora possam acometer, de forma direta e/ou indireta vítimas individuais, é comum a sua afetação ser refletida em custos para as entidades coletivas, alvos atrativos da ciber-criminalidade.

4.1. As vítimas de cibercrime e as consequências da experiência de cibervitimação

O impacto do cibercrime na vítima é muito variável, sendo agravado ou atenuado em função de um conjunto de:

- **Variáveis individuais**, nomeadamente características sociodemográficas e competências de utilização da Internet (já abordados nos fatores de risco associados à cibervitimação, no ponto 3 deste Manual);
- **Variáveis associadas ao cibercrime** propriamente dito, incluindo o tipo de cibercrime e nível de agressão subjacente, a duração da cibervitimação, o nível de audiência ou publicitação da cibervitimação e, nos casos em que se aplica, a relação com o/a autor/a do cibercrime (por exemplo, nas situações de cibervitimação no âmbito de relacionamentos interpessoais);
- **Variáveis associadas à rede de suporte**, no qual se inclui a rede de suporte formal (isto é, os recursos e serviços disponíveis por parte dos sistemas de justiça, de saúde, de segurança e proteção social, bem como por parte das organizações da sociedade civil), bem como a rede informal de apoio, nomeadamente familiares e amigos/as.

4.1.1. Consequências físicas, psicológicas e emocionais

Os estudos existentes relativos ao impacto e consequências da cibervitimação são escassos e, com raras exceções (e.g. Jansen & Leukfeldt, 2018), têm-se dedicado sobretudo a analisar os impactos de formas particulares de cibercrime, nomeadamente os crimes possibilitados pela Internet e pelas TIC, eventualmente pela componente relacional ou interpessoal que os encerra.

Em tudo mais, considera-se, genericamente, que as consequências experienciadas pelas vítimas de cibercrime não se distinguem de forma significativa das consequências experienciadas por vítimas de crimes que designaremos por *tradicionais*. As consequências e reações frequentemente apontadas

são: perda de confiança; culpa; vergonha; raiva e frustração; ansiedade; medo e tristeza; sentimentos de insegurança, impotência e desilusão (Leukfeldt et al., 2019; Cross et al., 2016; De Kimpe et al., 2020). O impacto emocional de certos tipos de cibercrimes pode ser tão severo quanto as consequências financeiras (Modic & Anderson, 2015). A vitimação também pode mudar a forma como as vítimas se percecionam e como entendem e atribuem significado ao mundo em seu redor, incluindo a redução nos níveis de autoconfiança e de confiança nas outras pessoas (Jansen & Leukfeldt, 2018), evoluindo posteriormente para efeitos físicos, como insónias, náuseas e/ou perda de peso (Cross et al., 2016).

Nas situações de *ciber-stalking*, o medo, a angústia e a preocupação sentidas pelas vítimas são consequências emocionais, psicológicas e comportamentais frequentemente identificadas (Holt & Bossler, 2008). O medo poderá dirigir-se ao/à autor/a dos atos de *ciber-stalking*, mas também associar-se ao receio de perda de reputação, pela possibilidade de informações pessoais e privadas serem divulgadas *online* e, como tal, alcançarem larga audiência ou elevada publicitação. A sintomatologia de ansiedade, incluindo re-experienciação dos incidentes vividos, e o consumo de substâncias também se associam à vitimação por *ciber-stalking*. A par das consequências emocionais e psicológicas, podem surgir indicadores de mal-estar físico, incluindo somatização[87], perturbações de sono, cansaço ou fraqueza excessiva, problemas de apetite, cefaleias e náuseas (Davies, Clark, & Roden, 2016).

Já nos casos de *ciber-bullying*, podemos elencar o sofrimento, a baixa autoestima, a tristeza, a raiva, a solidão e a frustração, assim como distúrbios somáticos, depressão e a ideação suicida como efeitos negativos frequentes no funcionamento psicológico e emocional da vítima. O *ciber-bullying* afeta ainda o funcionamento social e escolar da criança ou jovem vítima, estando associado a sentimentos de ineficácia, ao isolamento, ao absentismo escolar e ao declínio no desempenho académico (Beran & Li, 2007, Kowalski & Limber, 2013 *cit in* Arafa, Mahmoud & Senosy, 2015; Wang et al., 2011 *cit in* Arafa et al., 2015).

Por sua vez, estudos retrospetivos identificaram uma ampla gama de consequências negativas para o funcionamento emocional e psicológico associadas ao abuso sexual na infância, nomeadamente: dificuldades educacionais e ocupacionais, agressividade e envolvimento em atividades criminosas. Como havia sido identificado para as situações de *ciber-bullying*, também nas situações de abuso e exploração sexual de crianças é possível o surgimento de sintomatologia como o medo, ansiedade, agressividade e irritabilidade, assim como perturbações de sono e comportamentos regressivos[88]. Identicamente, pode haver lugar à diminuição do rendimento escolar e ao absentismo escolar, bem como à adoção de comportamentos sexuais desadequados (Roopesh, 2016 *cit in* APAV, 2019).

Não sendo o escopo do presente Manual a abordagem intensiva do abuso e exploração sexual de crianças e das suas consequências[89], atendendo à natureza atípica de algumas delas, apresentamos, em seguida, uma breve síntese dos referidos comportamentos sexuais desajustados que poderão surgir como consequências/efeitos da exposição a situações de violência sexual.

[87] A somatização diz respeito à manifestação de sintomatologia física sem razão médica/orgânica aparente como expressão de problemas emocionais e psicológicos.

[88] Comportamentos regressivos dizem respeito ao retrocesso em aquisições desenvolvimentais já alcançadas pela criança, nas quais se poderá incluir,por exemplo, a enurese (perda involuntária de urina), a encoprese (defecação involuntária) e retrocessos na linguagem/comunicação.

[89] Para informação adicional e detalhada sobre violência sexual contra crianças, queira consultar: APAV (2019). *Manual CARE - apoio a crianças e jovens vítimas de violência sexual (2.ª edição revista e aumentada).* Lisboa: APAV.

Quadro I-9: Comportamentos sexuais que podem surgir enquanto consequências de experiências de vitimação por violência sexual

Expressão sexualizada de afeto

- Toque inadequado nos órgãos sexuais de outras crianças e jovens (particularmente crianças e jovens de idades distintas da sua e/ou com as quais a criança ou jovem não tem relação prévia de confiança)
- Toque excessivo ou inadequado em pessoas adultas
- Condutas sedutoras para com pessoas adultas

Linguagem sexual precoce

- Utilização de termos sexuais indicativos de um conhecimento inesperado sobre sexualidade para a sua faixa etária

Masturbação compulsiva e/ou comportamentos autoeróticos extremos

- A masturbação persiste ainda que existam pedidos para parar ou, mesmo, censura por parte de pessoas adultas (ex.: aplicação de castigos consequentes à prática da masturbação)
- Masturbação em locais públicos e/ou junto de outras pessoas

Encenação ou simulação de episódios e/ou interações sexuais explícitas

Comportamento sexual gerador de mal-estar em si e nos outros (especialmente, nos pares)

- A conduta sexual provoca dor física em si e nos pares com os quais procura efetivar os atos sexuais
- A conduta sexual invade a privacidade e vontade dos pares e resulta em queixas destes últimos

Condutas sexuais concebidas como forma de retribuição/agradecimento de afeto e/ou bens materiais

Preocupação constante acerca do tema da sexualidade

Torna-se, deste modo, evidente que as situações de abuso e exploração sexual de crianças através da Internet afetam o seu desenvolvimento saudável, inclusivamente a nível sexual, bem como a identidade. Pelo elevado risco de vitimação continuada associado às situações de abuso e exploração sexual de crianças, são elevadas as probabilidades de o impacto da experiência aumentar na sua gravidade e de as consequências perdurarem até à idade adulta (Frothingham et al., 2000 *cit in* Sigurjonsdottir, 2013).

Por sua vez, nas situações de discursos de ódio *online* há lugar a um duplo impacto: o impacto do conteúdo/mensagem na vítima, mas também o impacto decorrente da mensagem subjacente que o mesmo conteúdo pretende transmitir (de que a vítima e o grupo ao qual ela pertence não são tolerados pela sociedade). Para além do anonimato garantido pela Internet e pela TIC aos/às agressores contribuir para a perpetuação da agressão *online* e, deste modo, para intensificar o sofrimento emocional e psicológico da vítima, o seu potencial de amplificação e "validação" social, nomeadamente quando a propagação decorre nas redes sociais, agrava e intensifica os impactos negativos provocados no funcionamento emocional, psicológico e mesmo social da vítima (McGonagle, 2013).

Já no caso de crimes ciber-dependentes, como o *hacking*, o *spamming* ou as burlas *online*, os impactos no bem-estar emocional e psicológico são, em larga medida, subestimados, sendo habitualmente concetualizados como crimes de baixo impacto (Button, Lewis, & Tapley (2014a *cit in* Jansen & Leukfeldt, 2018). No entanto, para lá das consequências financeiras associadas a estas formas de cibercrime, há estudos que apontam para a ocorrência de sintomatologia de desconforto emocional e psicológico, como medo e ansiedade, assim como sintomas físicos, como problemas de sono e palpitações (Jansen & Leukfeldt, 2018).

4.1.2. Consequências financeiras

O dano financeiro sofrido pelas vítimas de cibercriminalidade depende sobretudo das formas de cibercrime das quais foram alvo (Butler, 2013).

Poderão, por isso, ocorrer consequências financeiras diretas do cibercrime, assim como indiretas que podem incluir, por exemplo, outros custos suportados pelas vítimas como consequência do ato de que foram alvo, como o consumo de tempo, a perda de horas de trabalho, as despesas acrescidas com a saúde, os custos com deslocações e com telecomunicações, a necessidade de substituição de equipamentos de informática e/ou a falha no cumprimento de acordos contratuais (Leukfeldt et al., 2019). Há cibercrimes cujas consequências para a vítima se prendem ainda com a necessidade de alterar a sua rotina, o que pode implicar a adoção de medidas de segurança e a implementação de mecanismos mais eficazes de cibersegurança, mas também alterações mais significativas no estilo de vida e atividades quotidianas, incluindo mudança de casa, a alteração de local de trabalho/estudo ou outras, que obviamente acarretam custos financeiros.

Por outro lado, os custos que as entidades suportam como resposta ou consequência da cibercriminalidade da qual sejam alvos, aspeto explorado no campo 4.3 deste Manual, acabam por ser refletidos a nível individual, nos/as consumidores/as ou utilizadores/as *online* de um determinado produto, bem ou serviço (Das & Nayak, 2013).

4.1.3. Medo do cibercrime e risco percebido de cibervitimação

O **medo do crime** pode ser definido enquanto reação emocional ao crime e/ou a símbolos a ele associados, ao passo que o **risco percebido** constitui um julgamento cognitivo no qual as pessoas avaliam o seu próprio risco ou probabilidade de vitimação, em função das suas experiências pessoais, do contexto/ambiente social e das circunstâncias, o que, por sua vez, se reflete no medo relativamente ao crime (Ferraro, 1995, Rontree, 1998 *cit in* Yucedal, 2010).

Desta forma se depreende que as **experiências pessoais de vitimação** podem aumentar o risco percebido de (re)vitimação e, consequentemente, o medo face ao crime. Estes processos cognitivos não são necessariamente negativos, na medida em que podem promover a adoção de medidas e comportamentos de segurança e proteção (Rountree & Land, 1996, *cit in* idem).

Ora vejamos:

- Uma pessoa que já foi vítima de crime ou que se considera em risco de vitimação poderá **adotar mais comportamentos de segurança e proteção**, no qual se poderão incluir restrições nas atividades/interações sociais ou mudança nos hábitos diários, assim como o recurso a ferramentas e mecanismos de segurança;
- Uma pessoa que já foi vítima de crime pode percecionar-se em **maior risco de (re)vitimação** e, como consequência, apresentar níveis mais elevados de **medo face ao crime**, comparativamente aos índices de medo face ao crime de pessoas sem experiências prévias de vitimação (Hindelang et al., 1978, Cohen & Felson, 1979, Ferraro, 1995, Goodrum, 2007 *cit in idem*).

Estes **processos cognitivos de avaliação do risco percebido de vitimação também se aplicam à cibervitimação**: a perceção de risco de cibervitimação, como resultado de processos cognitivos que contemplam a análise das experiências pessoais de cibervitimação anterior (caso existam) e das pistas de vitimação/crime que advêm do estilo de vida *online*, poderá derivar em respostas comportamentais orientadas para uma maior proteção, nas quais se poderão incluir a implementação de medidas/mecanismos de cibersegurança (como programas anti vírus e *firewall*[90]) e a alteração dos comportamentos de utilização da Internet e das TIC (Yucedal, 2010).

Em última instância, o risco percebido de cibervitimação impacta também os níveis de **vulnerabilidade à cibervitimação**, uma vez que, à partida, se uma determinada pessoa se percecionar em risco de cibervitimação adotará, com maior probabilidade, comportamentos e medidas orientadas para a sua cibersegurança, o que contribuirá para a redução do risco de cibervitimação.

DESTAQUE | ESTATÍSTICAS EM FOCO:

De acordo com os dados do já mencionado Eurobarómetro 423, os/as inquiridos/as expressaram **elevados níveis de preocupação com a cibersegurança e com os riscos de cibercrime**.

Apresentamos, em seguida, alguns dos principais resultados recolhidos:

- A maioria (85% dos/as inquiridos/as) referiu concordar com o facto de o **risco de cibervitimação estar a aumentar**.
- 73% dos/as inquiridos/as referiram **recear que as suas informações pessoais *online* não sejam mantidas em segurança**.
- De entre a preocupação dos/as inquiridos/as face a diferentes tipos de cibercrime, destacou-se, por ordem decrescente, o **furto de identidade *online*** (68%), o ***malware*** (66%), as **burlas *online*** (entre 56% e 63%), o ***hacking*** (60%) e o ***spamming*** (57%). Por sua vez, cerca de metade dos/as inquiridos/as referiu preocupar-se com a descoberta acidental de **material de abuso e/ou de exploração sexual de crianças *online*** (52%) e com a descoberta acidental de conteúdos/material de incitamento aos **discursos de ódio** (46%).

Apesar destas preocupações, cerca de 74% referiram ser **capazes de se proteger contra o cibercrime**.

[90] *Firewall* diz respeito a *software* e/ou a *hardware* que tem como objetivo de proteger o computador/equipamento e rede face a acessos não autorizados.

4.2. Das consequências às necessidades das vítimas de cibercrime

De uma forma geral, as necessidades das vítimas de cibercrime são caracterizadas como relativamente semelhantes às necessidades das vítimas de outras formas mais *tradicionais* de criminalidade, sendo possível a identificação de diferentes domínios de necessidades (Leukfeldt et al., 2020).

Sendo certo que poderão ser indicadas necessidades mais ou menos comuns a vítimas de qualquer forma de crime, existirão necessidades que são específicas e diferem em função do tipo de vitimação e dos constrangimentos temporais (isto é, as necessidades de uma vítima de cibercrime imediatamente após a experiência de cibervitimação serão, à partida, distintas das necessidades identificadas algum tempo depois de o cibercrime ter ocorrido).

Ressalve-se, adicionalmente, que as necessidades das vítimas de crime dependem também das características pessoais da vítima, do ambiente social da vítima e das consequências do cibercrime de que foi alvo (Huang, 2018, Wood et al., 2015 *cit in idem*).

Não sendo exaustivo, inclusivamente atendendo à escassez de investigação sobre esta matéria, o quadro seguinte sumariza algumas das necessidades identificadas pelas vítimas de cibercriminalidade e que serão provocadas pela experiência de cibervitimação (Cross et al., 2016; Leukfeldt et al., 2020).

Quadro I-10: Necessidades identificadas pelas vítimas de cibercrime

Necessidades emocionais e psicológicas	Necessidades relacionadas com o processo-crime e de informação	Necessidades práticas e financeiras
• Reconhecimento enquanto vítima de um crime • Reconhecimento da experiência de cibervitimação • Necessidade de contar a sua experiência e de esta ser ouvida/escutada • Valorização externa (contextos sociais informais e autoridades) da experiência de cibervitimação • Obtenção de apoio qualificado e confidencial após a experiência de cibercrime • Recuperação das consequências emocionais e psicológicas decorrentes do cibercrime • Acesso a apoio profissional/qualificado	• Informação sobre os recursos/estruturas de apoio existentes e como pedir ajuda • Apoio na denúncia e formalização de queixa • Receber informação sobre o/a autor/a do cibercrime, sobre a investigação e julgamento • Receber informação sobre o desfecho/resultado do processo-crime • Reparação face ao crime	• Apoio na remoção do conteúdo relacionado com o cibercrime da Internet e das TIC • Apoio na articulação com entidades bancárias, ISP (*Internet Service Providers*) e outras plataformas • Apoio no restabelecimento da segurança (preservação da integridade física) e na prevenção da revitimação • Proteção/Afastamento face ao/à autor/a do cibercrime • Necessidades financeiras associadas aos bens/informações perdidas • Compensação monetária face aos prejuízos do cibercrime

A forma como as respostas institucionais proporcionadas pelos diversos sistemas e estruturas, como o sistema de justiça criminal, o sistema de saúde, o sistema de apoio e proteção social, os ISP (*Internet Service Providers*), a Indústria/Tecnologia, bem como as organizações da sociedade civil, intervêm ou atuam, tendo em vista a satisfação das necessidades das vítimas de crime e das vítimas de cibercriminalidade em particular, pode dar lugar a fenómenos de **vitimação secundária**. Trata-se de uma segunda forma de vitimação, provocada pela resposta inadequada providenciada por esses sistemas e estruturas e pela sua discrepância face aos interesses, necessidades e direitos das vítimas.

DESTAQUE | PRÁTICAS EM FOCO:

No que diz respeito à cooperação interinstitucional, como exemplo, veja-se a WePROTECT Global Alliance, pois propõe uma resposta coordenada, a nível nacional, em matéria de abuso e exploração sexual de crianças através da Internet.

O modelo proposto reconhece que o abuso e exploração sexual de crianças através da Internet constitui um problema que não pode ser intervencionado de forma isolada e que diferentes capacidades e competências são necessárias para o seu combate e prevenção.

Informação adicional em https://www.weprotect.org/.

As dificuldades dos diferentes sistemas/serviços e estruturas institucionais na resposta às necessidades das vítimas de cibercriminalidade (*idem*) podem dever-se aos seguintes constrangimentos:

- Insuficiência de recursos humanos e materiais;
- Desconhecimento sobre as necessidades e direitos das vítimas ou dificuldades estruturais para os implementar;
- Necessidade de formação/conhecimento especializado para o contacto e atuação junto de vítimas de cibercrime;
- Dificuldades associadas ao processo-crime, incluindo identificação de suspeito, formalização de queixa, investigação e acusação.

4.3. Custos financeiros e económicos do cibercrime

O cibercrime, nomeadamente nos casos em que atinge entidades coletivas enquanto alvos, representa custos variados para diferentes entidades. A magnitude dos custos económicos e financeiros do cibercrime varia de acordo com o setor, com a dimensão da entidade, com os ativos de informações e com a gravidade da(s) forma(s) de cibercrime de que foram alvo (Gañán, Ciere & van Eeten, 2017).

O cibercrime, quando dirigido a entidades coletivas, nomeadamente empresas e organizações, visa, sobretu-

do no caso de entidades de maior dimensão, atingir os seus ativos de informação. Já as entidades de menor dimensão parecem constituir-se como alvos menos atrativos da cibercriminalidade (Gañán et al., 2017).

No entanto, quando falamos sobre os custos económicos e financeiros da cibercriminalidade para as entidades, muitos desses impactos são **efeitos intangíveis** e não propriamente a perda de dinheiro real. Embora a necessidade de estimativas monetárias abrangentes seja compreensível, o impacto económico e financeiro da cibercriminalidade é difícil de mensurar, já que alguns dos efeitos podem ser monetizados, com base nos dados empíricos disponíveis, mas muitos deles não (*idem*).

Os vários tipos de custos associados ao cibercrime podem ser classificados como custos de antecipação, custos como consequência ou custos de resposta (*idem*).

Assim, nos custos de antecipação e nos custos como consequência, poderão incluir-se os custos (*a priori* e/ou *a posteriori*) com a **identificação de riscos**, a construção de **procedimentos operacionais de cibersegurança** e a aquisição de ***software* e *hardware* de proteção** contra o cibercrime. Poderão ainda inserir-se as despesas de consultoria especializada em matéria de cibersegurança, assim como custos associados à testagem, monitorização e atualização regular de riscos, procedimentos e sistemas de cibersegurança (Das & Nayak, 2013).

Já nos custos de resposta, incluir-se-ão todos os **gastos e esforços do setor público ou privado no combate ao cibercrime**, também suportados pela sociedade, incluindo os custos associados à intervenção do sistema de justiça criminal para a investigação e combate à cibercriminalidade (Gañán et al., 2017).

DESTAQUE | INFORMAÇÃO EM FOCO:

Impacto do cibercrime na confiança dos/as utilizadores/as

Os custos de antecipação são fundamentais para assegurar a confiança e segurança de utilizadores/as e consumidores/as na Internet e nas TIC.

A conveniência, a acessibilidade e a segurança associadas à utilização da Internet e das TIC para o consumo e aquisição de produtos, bens e serviços estão na base da preferência dos/as consumidores/as pelo comércio eletrónico e pelas atividades *online*, em comparação, por exemplo, com as lojas físicas.

A cibercriminalidade compromete as vantagens associadas à utilização da Internet e das TIC, aumentando os **índices de risco percebido** por parte dos/as utilizadores/as e consumidores/as *online*, reduzindo os níveis de confiança e contribuindo, deste modo, para a modificação das atitudes face ao consumo *online*.

Se a perceção de risco face à cibercriminalidade comprometer a confiança dos/as utilizadores/as ou consumidores/as relativamente à utilização da Internet e da TIC para determinadas atividades, a atratividade dos contextos *online* para o consumo e aquisição de produtos, bens e serviços diminui, o que, por seu turno, altera os hábitos e comportamentos *online* (Saban, McGivern & Saykiewicz, 2002; Smith, 2004; Saini, Rao & Panda, 2012).

PARTE II
PROCEDER

PARTE II
PROCEDER

1. O PAPEL DO/A PROFISSIONAL NO APOIO A VÍTIMAS DE CIBERCRIME

Neste capítulo do Manual, abordaremos a importância e o papel do/a profissional na prestação de apoio a vítimas de cibercrime, bem como as competências requeridas para o exercício de tais funções. Exploraremos, igualmente, os riscos psicossociais associados às exigências da intervenção com vítimas de crime, com particular enfoque nas vítimas de cibercrime.

1.1. Competências pessoais

O apoio a vítimas de crime e, neste caso em particular, de cibercrime, exige ao/à profissional de apoio um conjunto de competências essenciais e imprescindíveis.

As **competências pessoais** dizem respeito às características pessoais e à personalidade do/a profissional e ao modo como estas se adequam às funções e tarefas associadas à missão de apoio. Estas competências são primordiais em qualquer profissão de natureza assistencial, assumindo-se, por isso mesmo, como particularmente determinantes para os/as profissionais que trabalham no contacto e apoio direto a pessoas em dificuldade ou em situação de crise (APAV, 2013), de que podem ser exemplo as vítimas de cibercrime.

Assim, algumas das principais competências necessárias para o/a profissional que atua no domínio do apoio e intervenção com vítimas de crime - como a empatia, a abertura e a disponibilidade - são destacadas em seguida (Pessoa, da Mota Matos, Amado & Jäger, 2011).

Além destas competências, é **expectável ainda que o/a profissional seja capaz de gerir e estabelecer relações** interpessoais positivas no âmbito do apoio a vítimas de crime, o que inclui o contacto e interação com vítimas, seus familiares e amigos/as, bem como a articulação com profissionais e entidades parceiras que possam estar implicadas no apoio e intervenção com a vítima, em cada caso em particular. Nesta dimensão relacional, de gestão de relações humanas, inclui-se a capacidade de **resolução pacífica de problemas interpessoais e/ou interinstitucionais e a gestão positiva de *stress***. Estas características são bons indicadores da capacidade de se relacionar com o outro, sobretudo num contexto de intervenção naturalmente complexo e exigente, no qual o/a profissional é exposto a constantes adversidades (APAV, 2013; APAV, 2017).

Identicamente, a **autogestão emocional**, que diz respeito à capacidade de gerir e regular as suas emoções, perante situações de *stress*, frustração e exigência, em cenários totalmente díspares da sua realidade, representa competência fundamental (APAV, 2013). O contacto e intervenção com vítimas de crime envolve níveis elevados de exigência emocional, precipitados pelas experiências de violência/crime partilhadas pelas pessoas apoiadas/intervencionadas, pelo desenvolvimento e evolução do apoio em cada caso (e *stress* e frustração a ele associado) e pelos seus efeitos no equilíbrio emocional dos/as profissionais (APAV, 2017).

O/A profissional deve também demonstrar **tolerância e respeito pelos valores e diferenças cultu-**

[37] PInformação adicional em https://www.stopbullying.gov/.

[38] Informação adicional e detalhada sobre o estudo está disponível em: 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.

rais: independentemente de quaisquer características ou posicionamentos da vítima, a abordagem do/a profissional deverá ser sempre de abertura e aceitação. A neutralidade e imparcialidade são fulcrais para o melhor desempenho da missão de apoio, devendo o/a profissional procurar conter a interferência de valores e crenças pessoais no apoio a prestar junto de qualquer vítima (*idem*). Em associação com a dimensão anterior, na base de qualquer processo de apoio com vítimas de crime, está o **respeito pela dignidade humana**, sendo fundamental a aceitação incondicional da vítima enquanto ser humano, simultaneamente, semelhante a si próprio, mas também único e individual.

Por fim, e não menos importante, importa aludir a duas dimensões-base no contacto e apoio a vítimas de qualquer crime:

- **Compaixão e Empatia:**

  A capacidade para se colocar no *lugar da outra pessoa* ou de se imaginar na sua pele e na situação que descreve é fundamental no contacto, apoio e intervenção com vítimas de qualquer crime. A capacidade para se colocar na perspetiva da vítima de crime, de ser sensível à situação por ela vivenciada e de intuir e compreender os sentimentos e significados que atribui ao crime são importantes para o estabelecimento de uma **relação de apoio e de confiança entre profissional e vítima** e poderá ser um auxílio importante para o sucesso do apoio e/ou intervenção.

  Empatia não significa que o/a profissional deva chorar ou emocionar-se com aquilo que a vítima descreve sobre a situação de crime, sendo importante a já referida capacidade de autogestão emocional do/a profissional. Este equilíbrio é muito importante, para que a vítima de crime reconheça o/a profissional como uma figura de referência, preparada e qualificada para a função que desempenha (APAV, 2017; APAV 2019).

- **Vocação:**

  Ainda que não se trate propriamente de uma competência, mas de uma condição pessoal, a vontade e defesa pessoal dos valores de solidariedade social são muito importantes para a dedicação ao apoio, informação e/ou intervenção com vítimas de qualquer crime (APAV, 2017).

1.2. Competências técnicas de base e outras competências técnicas específicas

Para além das competências pessoais mencionadas anteriormente, o/a profissional que contacta e presta apoio a vítimas de crime e, em particular, de cibercrime deve estar devidamente qualificado/a para o efeito e para as funções que desempenha, assumindo-se também que as mesmas se deverão identicamente enquadrar no trabalho de uma determinada instituição, pública ou privada, governa-

[1] PORDATA, Indicadores de Envelhecimento, Índice de Envelhecimento 2018 https://www.pordata.pt/Portugal/Indicadores+de+envelhecimento-526 (consultado a 26-02-2020)

[2] Conselho Nacional de Ética para as Ciências da Vida, "Parecer 80/CNECV/2014 sobre as vulnerabilidades das pessoas idosas, em especial das que residem em instituições" (2014) https://www.cnecv.pt/admin/files/data/docs/1413212959_Parecer%2080%20CNECV%202014%20Aprovado%20FINAL.pdf (consultado a 27-02-2020)

mental ou não-governamental, de voluntariado social ou não (APAV, 2013).

A **formação de base** (ou seja, as habilitações académicas associadas à posse de um ou mais graus académicos) numa determinada área científica (como as ciências sociais, por exemplo, ou outra área, em função do tipo de apoio prestado pelo/a profissional e/ou pela entidade na qual exerce funções) a e a **experiência profissional** acumulada são aquisições importantes para a intervenção com vítimas qualquer crime, incluindo o cibercrime, nas suas diferentes formas de expressão (APAV, 2017).

Assim, é expectável que, de acordo com as necessidades identificadas em cada vítima e com a natureza do apoio solicitado, determinados profissionais sejam mais adequados, para a melhor resposta aos interesses, necessidades individuais e direitos de cada vítima de crime. Desta forma, torna-se claro que, por exemplo, o apoio ao nível jurídico deverá ser facultado por profissionais especializados na área do Direito e que, por seu turno, o apoio psicológico deverá ser prestado por Psicólogos/as devidamente habilitados/as[91].

Importa ainda salientar que, considerando a diversidade de necessidades e consequências habitualmente sentidas pelas vítimas de cibercrime[92], a a**poio e intervenção serão necessariamente interdisciplinares**, o que poderá implicar a atuação de profissionais de diferentes áreas de formação, bem como a intervenção de diferentes entidades. O trabalho realizado em rede, com profissionais e entidades com diferentes conhecimentos e *know-how* e de âmbitos/setores de intervenção distintos, contribui para uma melhor intervenção junto de cada vítima de cibercrime e para a adequada satisfação das suas necessidades individuais.

Complementarmente à formação superior e à experiência profissional, o/a profissional que contacta ou apoia vítimas de cibercrime deverá deter também **formação específica**, regular e contínua, em matéria de intervenção com vítimas de crime e de cibercrime, bem como ao nível da cibercriminalidade enquanto domínio específico de conhecimento (APAV, 2013; APAV, 2017). Nesta formação específica, deverá considerar-se, de forma não exaustiva, os seguintes conteúdos-chave: a compreensão teórica, criminológica e vitimológica das diferentes formas de cibercrime; o conhecimento sobre as consequências, impactos e dinâmicas da cibervitimação, bem como sobre as necessidades e direitos das vítimas; o enquadramento jurídico e as respostas legais e sociais existentes; a cibersegurança; entre outros conteúdos.

Adicionalmente, atendendo à natureza da cibercriminalidade e aos mecanismos contra os quais (ou através dos quais) o crime é praticado, o contacto e apoio a vítimas de cibercrime obriga também ao **conhecimento e formação especializada relativo à Internet, às TIC e demais equipamentos**, tanto no que respeita ao funcionamento destes últimos e das ferramentas de comunicação suportadas pela Internet (nas quais se incluem as redes sociais), como no que se refere ao modo como podem ser utilizadas para a prática de crimes e/ou como podem constituir, em si mesmo, alvos da cibercriminalidade (Bloom, 2007, Poh et al., 2013, Trepal et al., 2007, Mallen, Vogel, & Rochlen, 2005 *cit in* APAV, 2017). A **proficiência informática e tecnológica** do/a profissional é fundamental para a

[91] Veja-se ponto 3.5. do capítulo 3 da parte II deste Manual, para informação sobre os aspetos fundamentais do apoio especializado junto de vítimas de cibercrime.

[92] Veja-se capítulo 4 da Parte I deste Manual, para mais informações sobre esta matéria.

capacidade de acompanhar a constante evolução das TIC, das tendências de comunicação através da Internet, bem como a permanente e consequente mutação da cibercriminalidade.

Não menos importantes serão as **competências comunicacionais** no contacto e apoio a vítimas de cibercrime, nomeadamente, saber ouvir/escutar, mas também ter a capacidade para transmitir informação e mensagens claras e inteligíveis, no âmbito do processo de apoio, em torno de temáticas que bem sabemos que são complexas (Pessoa et al., 2011). A comunicação e a empatia, enquanto base do processo de apoio e da relação entre profissional e vítima de cibercrime, serão abordadas, em maior detalhe, nos pontos seguintes deste Manual.

1.3. Os riscos psicossociais associados ao contacto e apoio a vítimas de cibercrime

O/A profissional que contacta, apoia e/ou intervém com vítimas de crime, pelas funções que desempenha e pela necessidade de contacto direto com pessoas em situação de particular vulnerabilidade e fragilidade (inclusivamente emocional, mas também física) causadas pela vitimação e cibervitimação, apresenta níveis elevados de **desgaste físico e emocional, de sofrimento psicológico e de *stress* ocupacional**. Não só estes/as profissionais são expostos às experiências pessoais de vitimação de outras pessoas, como são confrontados/as com as frustrações associadas ao desequilíbrio entre as expectativas de resolução/satisfação dos problemas e necessidades apresentadas pela vítima e o funcionamento e recursos disponibilizados pelo sistema e pelas estruturas institucionais. Adicionalmente, para lá da exposição *convencional* ao relato das vítimas relativamente às suas experiências pessoais de vitimação (veja-se pontos seguintes deste Manual, nos quais detalharemos a importância da recolha de informação), no caso do/a profissional dedicado ao apoio a vítimas de cibercrime, a essa exposição poderá adicionar-se uma outra dimensão potencialmente causadora de stress ou trauma, que respeita à necessidade de visualizar conteúdo, seja através de imagens, fotografias e/ou vídeos, de natureza criminal associada às formas de cibercrime que foram/são praticadas contra a vítima que se encontra a ser apoiada: esse conteúdo poderá ser de natureza marcadamente agressiva, violenta e mesmo sexualmente explícita (como é o caso do apoio a crianças e jovens vítimas de abuso e/ou de exploração sexual através da Internet, do apoio a vítimas de *ciber-stalking* ou do apoio a vítimas de extorsão sexual ou de divulgação não consensual de imagens e vídeos, como ocorre nas situações de *revenge porn*[93]). A exposição contínua a este tipo de conteúdo potencialmente traumático poderá comprometer o bem-estar e funcionamento do/a profissional de apoio (McCann & Pearlman, 1990).

Não é, por isso, incomum o surgimento de situações de *burnout* que se define, sinteticamente, como uma síndrome (ou constelação de sintomas), na qual se incluem sintomas de **exaustão emocional, despersonalização**[94] e **baixa realização pessoal**, manifestada mediante situações de trabalho causadoras de *stress* (Campos, Jordani, Zucoloto, Bonafé & Maroco, 2012).

[93] Para informação detalhada sobre estas formas de cibercrime, queira consultar capítulo 1 da parte I deste Manual.

[94] Por despersonalização entende-se o processo de desumanização no trato/contacto com o outro, manifestado através de interações interpessoais desprovidas de afetividade e empatia.

Não sendo exaustivo, o quadro seguinte sintetiza algumas medidas organizacionais e comportamentos individuais do/a profissional dedicado ao contacto ou apoio a vítimas de cibercrime, tendo em vista a prevenção dos riscos psicossociais associados ao apoio a vítimas de crime e de cibercrime.

Quadro II-1: Medidas de prevenção de riscos psicossociais associados ao apoio a vítimas de crime e de cibercrime

Medidas organizacionais da entidade com respostas/ serviços de apoio para vítimas de cibercrime	Comportamentos individuais de profissionais dedicados ao contacto e apoio a vítimas de cibercrime
• Promover uma cultura organizacional de abertura ao *feedback* e à partilha de experiências • Fornecer acesso a mecanismos ou respostas de apoio psicológico específico, interno e/ou externo, destinado aos/às profissionais de apoio • Implementar mecanismos de aconselhamento relacionados com o bem-estar dos/as profissionais de apoio, através de modalidades individuais e/ou grupais • Realizar reuniões regulares para discussão e partilha de experiências/casos entre pares/equipa/profissionais de apoio • Promover espaços de trabalho com recursos materiais e logísticos condizentes com a atividade e promotores de bem-estar • Promover atividades lúdicas e de lazer não relacionadas com tarefas e funções habitualmente executadas pelos/as profissionais de apoio	**Comportamentos de autocuidado:** • Praticar exercício físico • Praticar atividades de lazer • Reconhecer e respeitar as normas básicas de saúde, mantendo uma dieta equilibrada e boa higiene de sono • Manter contacto com a família e amigos/as • Reconhecer e respeitar os limites do corpo e mente • Garantir tempos e momentos de descanso e desconexão com o trabalho, através de atividades prazerosas • Recorrer a técnicas de relaxamento e meditação • Ter contacto com a natureza **Técnicas de intervenção:** • Aceder a apoio psicológico, disponibilizado na entidade no qual o contacto ou apoio a vítimas de cibercrime é realizado ou externamente • Participar em momentos de aconselhamento individual e/ou de grupo (entre equipa/pares)

[37] PInformação adicional em https://www.stopbullying.gov/.

[38] Informação adicional e detalhada sobre o estudo está disponível em: 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.

2. ASPETOS-CHAVE NO CONTACTO COM VÍTIMAS DE CIBERCRIME

Este capítulo será dedicado a um conjunto de orientações gerais para o contacto com vítimas de cibercrime e precede uma intervenção mais estruturada e de qualidade junto de qualquer vítima de cibercrime, independentemente da entidade no qual o contacto com a vítima de cibercrime seja efetuado.

Para o efeito, destacamos dimensões-chave para o estabelecimento de uma relação de confiança entre a vítima e o/a profissional de apoio, incluindo a comunicação e a empatia, mas também a recolha de informação e o modo como a mesma orientará qualquer intervenção subsequente junto da vítima de cibercrime. Este capítulo termina com uma abordagem aos cuidados a ter no contacto com crianças e jovens vítimas de cibercrime, atendendo à sua particular vulnerabilidade.

2.1. Orientações gerais para o contacto com vítimas de cibercrime

A procura de apoio por parte de uma vítima de cibercrime pode representar um momento-chave e determinante para a sua recuperação emocional e psicológica e para o restabelecimento da normalidade da sua vida.

No entanto, como em outros crimes, também nas situações de cibercriminalidade, só uma proporção, ainda que diminuta e cuja dimensão exata carece de aferição, de vítimas opta pela procura de apoio formal, nomeadamente junto dos serviços e respostas de apoio a vítimas. Pese embora a relutância frequente na procura de apoio (Cross et al., 2016), por motivos que se entrecruzam com os da não denúncia do cibercrime[95], por norma, o pedido de apoio dependerá de duas condições: que as vítimas de cibercrime se reconheçam, de facto, enquanto vítimas de um crime e que avaliem o cibercrime sofrido enquanto grave (De Kimpe et al., 2020).

Apresentamos, em seguida, algumas orientações globais para a atuação do/a profissional no apoio a vítimas de qualquer crime, incluindo vítimas de cibercrime (Winkel, 1991; Machado & Gonlçalves, 2003 *cit in* APAV, 2013; Cross, Richards & Smith, 2016; Wedlock & Tapley, 2016; De Kimpe, Ponnet, Walrave, Snaphaan, Pauwels & Hardyns, 2020).

[95] Veja-se ponto 1.4. do capítulo 1 da parte I deste Manual, para informação mais detalhada sobre as cifras negras associadas ao cibercrime.

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

Objetivos	Atitudes
Valorizar a denúncia	Reforçar a coragem da procura de apoio e da revelação da experiência pessoal de cibervitimação.
Respeitar o ritmo da vítima & promover a partilha da sua experiência	Privilegiar o recurso a questões abertas, como "o que tem para nos contar?", promovendo um espaço/contexto seguro para a partilha livre de informação. Respeitar e promover a ventilação emocional, bem como momentos de maior fragilidade e emocionalidade associados à partilha da experiência de cibercrime. Questionar, sem pressionar, quando a informação fornecida pela vítima é pouco clara ou insuficiente. Respeitar os tempos, as pausas e os silêncios da vítima, incluindo as hesitações na partilha de informação.
Validar a experiência	Escuta empática, demonstrando que está a escutar e a compreender o que está a ser dito e a valorizar as reações, emoções/sentimentos, comportamentos, pensamentos e significados atribuídos pela vítima à sua experiência de vitimação/cibervitimação. Demonstrar que acredita naquilo que a vítima está a contar sobre o que lhe aconteceu, sem julgamentos ou juízos de valor. Normalizar as reações apresentadas.
Reestabelecer o controlo	Informar, de forma inteligível, transmitindo informação essencial à vítima sobre o que aconteceu e os passos seguintes a adotar, através de linguagem simples, clara e ajustada às características da vítima. Não substituir a vítima na tomada de decisões, aceitando-as sem julgamento e orientando a sua implementação/efetivação, tendo em vista o restabelecimento do controlo sobre a sua vida. Respeitar as escolhas da vítima.
Romper com a ideia de "vulnerabilidade única"	Fornecer informações sobre o crime e sua prevalência.
Prevenir a culpabilização	Não criticar. Enquadrar as reações da vítima no contexto emocional do ato. Valorizar tentativas prévias de proteção, ainda que possam ter sido ineficazes. Evitar a utilização de expressões do tipo "porque é que não..." e "devias ter...".
Prevenir o evitamento e o isolamento	Recomendar o retomar progressivo de atividades, incluindo hábitos de utilização da Internet e TIC. Incentivar o reforço do envolvimento em atividades anteriormente apreciadas, nomeadamente as atividades *offline*. Mobilizar o suporte social. Evitar a hiperproteção por familiares e amigos/as (sem negligenciar a segurança da vítima).
Promover o processamento emocional e cognitivo da experiência	Não aconselhar a vítima a "esquecer tudo" e recomendar às pessoas próximas que não o façam. Sugerir a partilha de sentimentos e receios com aqueles/as em quem confia, recomendando aos últimos que mantenham uma posição de disponibilidade para a escuta, sem pressionarem à partilha.
Prevenir novos crimes	Discutir estratégias de segurança e de cibersegurança. Consciencializar para os riscos associados à utilização da Internet e das TIC, promovendo a implementação de mecanismos de cibersegurança e a adoção de comportamentos de proteção pessoal aquando da utilização da Internet e das TIC. Elaborar, se necessário, um plano de segurança com a vítima (nomeadamente nas situações em que a cibervitimação é acompanhada por vitimação nos contextos *tradicionais*).
Envolver pessoas significativas no processo de recuperação	Caso seja vontade da vítima e com a sua autorização, envolver familiares e/ou amigos/as no processo de recuperação, solicitando o seu auxílio para o apoio ao processamento da experiência, para a prevenção de novos crimes, do evitamento e do isolamento.

Complementarmente, apresentamos, em seguida, uma sistematização de boas práticas e de erros comuns a evitar no contacto com qualquer vítima de crime (APAV, 2019b).

Quadro II-3: Boas práticas vs erros a evitar no contacto com vítimas de cibercrime

Boas práticas no contacto com a vítima de cibercrime	Erros a evitar no contacto com a vítima de cibercrime
Acreditar no relato da vítima.	Não acreditar no relato da vítima.
Incentivar a vítima a falar sobre a situação de cibervitimação, contudo, sem a pressionar.	Substituir a vítima na tomada de decisão, erro habitualmente identificável por expressões do tipo "Você não deve", " Você deve".
Respeitar a confidencialidade, tendo em conta os seus limites.	Tomar decisões sem a autorização prévia da vítima.
Não emitir juízos de valor.	Oferecer à vítima uma falsa sensação de segurança e/ou promover expectativas irrealistas quanto ao seu papel e/ou quanto à resolução da situação e/ou das necessidades, o que pode ser visível através de verbalizações do tipo "Não se preocupe. Vai ficar tudo bem."
Respeitar a leitura que cada vítima apresenta da sua situação específica, mesmo que esta seja contrária à visão do/a profissional.	
Normalizar a experiência de cibervitimação e as variadas reações, emoções, sentimentos e pensamentos associados.	Minimizar o problema e o seu impacto.
Explicar à vítima que existem outras pessoas a viver situações semelhantes à sua, quebrando a noção de "caso único".	Adotar uma postura de hiperproteção em relação à vítima.
Transmitir à vítima que não é responsável pela situação, auxiliando-a a lidar com possíveis sentimentos de auto culpabilização.	Demonstrar interesse excessivo por detalhes da cibervitimação que a vítima não tenha vontade de revelar (ou que, naquele momento, ainda não esteja preparada para revelar).
Auxiliar a vítima no processo de decisão, demonstrando-lhe as vantagens e desvantagens de cada opção, tendo em vista a tomada de decisões informadas.	Demonstrar pouco tempo e/ou pouca disponibilidade para a vítima e para a escutar, através, por exemplo, de manifestações não-verbais de inquietação e/ou de interrupções ao seu discurso.
Avaliar o risco de ciber[re]vitimação e as necessidades da vítima, disponibilizar o apoio adequado, consoante a sua situação, e/ou encaminhando para os serviços e/ou entidades onde tal apoio possa ser providenciado.	Propor interpretações ou diagnósticos face a reações, emoções/sentimentos e pensamentos da vítima perante a sua experiência de cibervitimação, detetável em expressões como "Você está a fazer isso porque ...".
Estar preparado/a para intervir numa situação de crise.	Oferecer soluções, sem envolver a vítima no processo de decisão.
	Utilizar o humor de forma inapropriada ou fazer autorrevelações desnecessárias, como estratégias para o estabelecimento de uma relação de confiança.

2.2. A importância da comunicação e da empatia

A **empatia**, como referido anteriormente, caracteriza-se pela capacidade de compreender a perspetiva da outra pessoa e de perceber e apreender o que esta está a sentir atualmente, o que sentiu aquando da experiência de cibervitimação, o que pensa ou pensou relativamente ao acontecimento,

bem como pela capacidade de demonstrar o seu entendimento e validação perante o desconforto e mal-estar e demais reações, mais ou menos imediatas, subsequentes ao cibercrime.

A empatia do/a profissional relativamente à vítima e à sua experiência de cibervitimação é muito importante para o **estabelecimento de uma relação de apoio e de confiança entre profissional e vítima**, sendo certo que a execução bem-sucedida dos objetivos anteriormente elencados (veja-se Quadro 2) assenta, em larga medida, nos alicerces desta relação de confiança.

Desempenhando um **papel crucial na comunicação humana**, já que facilita o processo comunicacional, a empatia encoraja a vítima à partilha, inclusivamente de informação e meios de prova, o que contribuirá para o sucesso do processo de apoio, para a recuperação da vítima e para a resposta às suas necessidades, mas também beneficia o decurso do processo-crime (De Vignemont & Singer, 2006; Sommers-Flanagan & Sommers-Flanagan, 2014, Themeli, 2014, Morrison, 2014 *cit in* APAV, 2018).

DESTAQUE | INFORMAÇÃO EM FOCO:

A empatia não pode, no entanto, significar que o/a profissional se descontrole e chore com a vítima. Tal conduta ou reação poderá provocar, ainda que inadvertidamente, impacto negativo na vítima e na qualidade do processo de apoio, já que a vítima poderá deixar de entender o/a profissional como alguém qualificado e preparado para a prestação de apoio.

Alguns dos aspetos que o/a profissional deve contemplar na **comunicação empática** são (APAV, 2019b):

- Manter contacto ocular com a vítima, num registo apaziguador e não inquisidor.
- Acompanhar o contacto ocular por um tom de voz sereno e interessado e por linguagem corporal de disponibilidade e tranquilidade (por exemplo, evitando olhar para o relógio, evitar demonstrar qualquer sinal de impaciência ou realizar interrupções desnecessárias ao discurso da vítima).
- Recorrer a interjeições que reforcem e validem a partilha da experiência de cibervitimação por parte da vítima e a coragem na procura de apoio.
- Demonstrar claramente que está a escutar com atenção a informação que a vítima partilha, incluindo através da linguagem não-verbal (acenar afirmativamente, por exemplo).
- Garantir à vítima que está a compreender a informação por ela partilhada, através, por exemplo, de:

    - Reformulações – devolver à vítima, por palavras do/a profissional, o conteúdo por ela transmitido. A reformulação auxilia o/a profissional a ter a certeza de que compreendeu adequadamente a vítima, mas também garante/informa indiretamente a vítima de que está a ser ouvida com atenção, o que a encorajará a continuar.
    - Resumos – sintetizar a informação partilhada pela vítima, nomeadamente aquando do encerramento de um assunto/tópico, no final de uma sessão de apoio e/ou no início da

seguinte. Resumir pode ser um excelente modo de colmatar lacunas na informação e/ou desentendimentos quanto ao que foi realmente comunicado.

- Assegurar a vítima de que está interessado/a e envolvido/a no contacto/interação, através, nomeadamente, do questionamento. Deverá privilegiar-se o equilíbrio entre as questões abertas e as questões fechadas, o que facilita a comunicação espontânea e evita que a vítima se sinta interrogada. Para abordagens iniciais a novos assuntos/tópicos e, tendo em vista a partilha de informação, deverá optar-se por questões abertas. Já as questões fechadas permitem o acesso a informação concreta e específica.
- Encorajar a expressão emocional, sobretudo quando a pessoa está em situação de crise. Contudo, o/a profissional não a deverá impor a expressão emocional, caso a vítima não tenha manifestado vontade de o fazer.

2.3. A recolha de informação enquanto etapa-chave

A recolha de informação é um processo central para o apoio e intervenção junto de qualquer vítima de crime, incluindo vítimas de cibercrime.

Sendo certo que, à partida, o **primeiro contacto com a vítima será dedicado a este processo de recolha e reunião de informação** sobre o cibercrime, o seu impacto e as necessidades precipitadas, é importante manter presente que a **recolha e análise da informação constituem etapas circulares e constantes**, que alimentam regularmente qualquer processo de apoio e de intervenção com vítimas de crime e de cibercrime.

DESTAQUE | INFORMAÇÃO EM FOCO:

Não é incomum que a vítima demonstre **sinais de ansiedade e desconforto neste primeiro contacto com o/a profissional de apoio** e/ou com a entidade na qual o apoio é disponibilizado.

O/a profissional deve considerar que a vítima poderá estar, pela primeira vez, a partilhar informação sobre a sua situação de cibervitimação, sendo naturais os indicadores de mal-estar, de sofrimento e fragilidade, de hesitação e/ou de vergonha. Estes indicadores podem ser particularmente prevalentes quando a informação a partilhar contém algum tipo de detalhe relacionado com a intimidade relacional e/ou sexual da vítima.

O/A profissional deve (em linha com a informação sintetizada no Quadro 2):

- Respeitar os silêncios, hesitações e o ritmo da vítima.
- Reforçar a coragem da vítima na procura de apoio e na partilha de informação sobre a sua história de cibervitimação.
- Explicar e tranquilizar a vítima quanto à naturalidade das suas reações, emoções/sentimentos e pensamentos, tanto no que respeita ao desconforto face à partilha de informação em contexto de apoio, como

no que se refere à experiência de cibervitimação propriamente dita: em qualquer dos casos, tratam-se de reações naturais perante acontecimentos e circunstâncias de vida inesperadas ou anormais.
- Demonstrar-se disponível e presente para apoiar a vítima e para a escutar, incluindo os seus receios, preocupações e anseios.

A **recolha de informação deve ser ajustada ao estado emocional da vítima**, o que significa que, caso esta não esteja capaz de devolver toda a informação, o/a profissional deverá recolher a informação que for possível e, caso esta não seja suficiente, deverá ser promovida a existência de atendimentos/contactos posteriores que permitam uma recolha mais completa e profunda.

O bem-estar emocional da vítima deve ser priorizado, mesmo que em detrimento da necessidade de recolha de informação.

Sinteticamente, a recolha de informação junto da vítima de cibercrime permite ao/à profissional de apoio:

1
- **obter informação sobre a situação de cibercrime experienciada pela vítima**
- **aferir os impactos e consequências experienciadas pela vítima de cibercrime**

2
- **avaliar o risco de ciber(re)vitimação e de vitimação em geral**
- **definir medidas de cibersegurança e comportamentos de proteção pessoal online**

3
- **identificar as necessidades da vítima de cibercrime**
- **acionar os recursos e serviços mais adequados à resposta às necessidades da vítima e à resolução/minimização dos impactos da experiência de cibervitimação**

Figura II-1: Áreas/domínios a considerar na recolha de informação

A recolha de informação deverá ser dirigida a 3 domínios:

1. **História pessoal e de pré-vitimação**
   O/A profissional deverá procurar recolher informação sobre o contexto familiar, profissional e social. Deverá tentar avaliar possíveis episódios de vitimação anteriores, bem como os hábitos de utilização da Internet, das TIC e redes sociais, os comportamentos/atividades de risco, as medidas de cibersegurança adotadas ou a sua ausência, bem como os comportamentos de proteção pessoal *online*.

2. **Experiência de cibervitimação**
   Neste domínio, deverá procurar-se reunir toda a informação possível sobre a situação de cibercrime experienciada pela vítima, com detalhes sobre as circunstâncias, incluindo informação sobre o que aconteceu; como aconteceu; quais as TIC e/ou ferramentas de comunicação suportadas pela Internet utilizadas; junto de quem foram divulgadas/partilhadas evidências do cibercrime sofrido

e/ou através de que plataformas; quem são os/as autores/as e qual o nível de conhecimento entre vítima e autores/as; quando teve início a situação de cibervitimação e se é ou não continuada; se há ou não entrecruzamento entre cibervitimação e outras formas de vitimação *tradicional* envolvendo os/as mesmos/as autores/as ou outros/as; quais as medidas já acionadas pela vítima.

3. **História pós-vitimação**
   O objetivo prende-se com a análise e avaliação do impacto da cibervitimação, compreendendo as consequências, os mecanismos de *coping* colocados em prática, os fatores de proteção que a vítima dispõe, desde logo avaliando o suporte familiar e social e a capacidade que a mesma tem para gerir o impacto e adquirir novamente o controlo sobre a sua vida. Também será importante avaliar a motivação para a prática de medidas preventivas e definição de um plano de segurança.

2.4. O caso específico das crianças e jovens vítimas de cibercrime

Com abordado na parte I deste Manual[96], as crianças e jovens, pelos seus hábitos e comportamentos de utilização da Internet e das TIC, bem como pela dificuldade na supervisão de tais comportamentos por parte das pessoas adultas (nomeadamente do contexto familiar), constituem-se enquanto grupo vulnerável à cibervitimação.

O contacto e apoio a crianças e jovens vítimas de cibercrime deverá:

1. Pautar-se sempre pela **promoção e proteção dos seus direitos**;
2. Atender às características e **estádios de desenvolvimento** da criança ou jovem;
3. Contemplar, sempre que possível, o **envolvimento da família**;
4. Apresentar um enfoque na educação para uma utilização segura e consciente das TIC e da Internet, enquanto comportamento de proteção face à revitimação.

Abordaremos, em seguida, com maior detalhe, cada um destes pontos.

1

- **promover e proteger os direitos das crianças ao longo do contacto/apoio junto da criança/jovem vítima de cibercrime**

No contacto e apoio a crianças e jovens vítimas de crime em geral e, em particular, de cibercrime, deverá o/a profissional orientar sempre a sua atuação, tendo em vista a salvaguarda dos seus direitos.

[96] Veja-se ponto 3.2 de parte I deste Manual.

2. ASPETOS-CHAVE NO CONTACTO COM VÍTIMAS DE CIBERCRIME

Não pretendendo este Manual ser exaustivo nesta matéria, atendendo inclusivamente às especificidades e particularidades da legislação nacional de cada Estado-Membro, poderemos, genericamente, dizer que cada profissional que contacte ou apoie uma criança ou jovem vítima deverá conhecer a legislação em vigor[97] e definir a sua atuação em consonância.

A Convenção sobre os Direitos das Crianças[98], no qual se incluem um conjunto de direitos universais básicos aos quais todas as crianças deverão ter acesso, contempla alguns princípios fundamentais que se adequam a qualquer intervenção com crianças e jovens. Ora vejamos:

- **Superior interesse da criança** que, sucintamente, refere que todas as leis e ações que afetam as crianças devem colocar, em primeiro lugar, os seus interesses, beneficiando-as da melhor forma possível.
- **Não-discriminação**, princípio segundo o qual nenhuma criança deverá ser prejudicada (ou beneficiada) por causa da raça, cor, sexo, língua, religião, nacionalidade, origem étnica ou social, por causa de qualquer opinião política ou outra, condição económica, estatuto ou por qualquer limitação física ou mental.
- **Sobrevivência, desenvolvimento e proteção**, segundo os quais as autoridades devem proteger todas as crianças e ajudar a garantir o seu pleno desenvolvimento, a nível físico, social, espiritual e moral.
- **Participação**, segundo a qual todas as crianças têm o direito a ter uma palavra a dizer nas decisões que as afetam, assim como a ser ouvidas nos assuntos que lhes dizem respeito.

Assim, o/a profissional e a entidade na qual as suas funções são exercidas deverão estabelecer, definir e executar a sua intervenção de acordo com estes princípios e com a legislação relevante, tendo sempre em mente a necessidade de promover o **pleno exercício dos direitos das crianças e jovens**.

- **respeitar e considerar as características e estádios de desenvolvimento da criança ou jovem vítima ao longo do contacto/apoio**

2

O contacto e apoio a uma criança ou jovem vítima de cibercrime terá necessariamente de ser distinto do contacto ou apoio providenciado a uma pessoa adulta vítima de cibercrime.

O/a profissional deverá conhecer os principais marcos no **processo de desenvolvimento da criança ou jovem**, nomeadamente ao nível da linguagem e comunicação, uma vez que tal deverá refletir-se em modificações e adaptações a encetar pelo/a profissional nas estratégias de comunicação a utilizar junto da criança e jovem vítima, no decurso da sua atuação (APAV, 2019).

Não sendo exaustivo, o quadro seguinte apresenta sucintamente os principais marcos no desenvolvimento global da criança ou jovem, em função da faixa etária.

[97] No caso Português, a Lei n.º 147/99, de 1 de Setembro, relativa à Lei de proteção de crianças e jovens em perigo e alterações posteriores, tem por objeto a promoção dos direitos e a proteção das crianças e jovens em perigo, por forma a garantir o seu bem-estar e desenvolvimento integral. Veja-se diploma disponível em https://apav.pt/apav_v3/images/pdf/protecao_criancas_jovens_perigo.pdf.

[98] Veja-se texto completo em https://www.ohchr.org/en/professionalinterest/pages/crc.aspx.

Quadro II-4: Estádios-chave no processo de desenvolvimento da criança/jovem

	Desenvolvimento físico	Desenvolvimento emocional e cognitivo (incluindo linguagem)	Desenvolvimento social e moral
3-6 anos	• É capaz de desenhar e de outras manualidades • É capaz de escrever o seu próprio nome • O corpo desenvolve-se, assumindo as formas do corpo adulto • A destreza e capacidade de coordenação aumentam	• Lembra-se de experiências familiares • Possui algum vocabulário • É capaz de ajustar o discurso de acordo com as características do/a interlocutor/a (como idade, sexo e estatuto social)	• É capaz de interpretar, prever e influenciar as reações de outras pessoas • Estabelece as primeiras amizades • Surgem as emoções autoconscientes (como vergonha e culpa) • Tem um controlo relativo sobre as suas emoções
6-12 anos	• Aumenta progressivamente de peso e de altura • A caligrafia torna-se mais pequena e legível • Os desenhos são mais estruturados • Os jogos e brincadeiras que envolvam correrias, confusão e competição são comuns • Desenvolve-se a capacidade de resposta rápida ao nível da destreza motora • Podem evidenciar-se indicadores púberes, particularmente no caso das raparigas	• Os pensamentos e a capacidade de atenção são mais focalizados • Raciocínio indutivo • É capaz de estabelecer a relação entre experiências e ocorrências específicas • Aumento de vocabulário	• Torna-se mais independente e mais responsável • Faz a distinção entre ser bem-sucedido e malsucedido • Tem consciência dos seus esforços vs acaso/sorte na obtenção de um dado resultado • É capaz de se colocar no lugar do outro (empatia)
12-18 anos	• Puberdade • Menstruação e aumento do tecido adiposo, no caso das raparigas • Voz torna-se mais grave e há aumento de massa muscular, no caso dos rapazes • Maior interesse pela sexualidade	• É capaz de discutir eficazmente • É mais autoconsciente e concentrado/a • Desenvolvimento do raciocínio hipotético-dedutivo • É capaz de ajustes subtis no discurso • É capaz de fazer planos e de tomar decisões	• Aumento da conflitualidade com pais/família • Aproximação ao grupo de pares e aparecimento das situações de pressão de pares • Procura da própria identidade • Desenvolvimento de relacionamentos íntimos

Já o quadro seguinte procura explicitar algumas das diferenças essenciais na abordagem e comunicação com crianças e jovens de diferentes faixas etárias, aquando do contacto e apoio por parte do/a profissional (APAV, 2011).

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

	1-6 anos	6-12 anos	12-18 anos
Apresentação	Fundamentalmente dirigida à criança. É ainda demasiadamente nova para poder compreender a informação prestada.	A criança demonstra mais interesse na informação prestada e maior capacidade para a compreender. Apresenta mais detalhes do que as crianças mais novas.	Compreende a informação prestada mas pode demonstrar relutância quanto à participação num programa de intervenção ou num processo de apoio à vítima.
Descrição do acontecimento	Expressa-se preferencialmente através de desenhos ou de jogos, preterindo a expressão verbal.	As crianças mais velhas preferem expressar-se verbalmente recusando, por vezes, o recurso a desenhos e jogos.	A descrição do acontecimento é detalhada. Verificam-se sentimentos de auto-culpabilização.
Psico-educação	Fundamentalmente dirigida à família/pais. No entanto, a criança assimilará informações simples, como o reconhecimento da situação, pelo que poderá simular uma maneira de lidar com ela.	Dirigida à criança, integrando a família/pais no processo de psico-educação.	Dirigida à/através da criança.

Adicionalmente, importa que o/a profissional, no contexto do contacto ou do apoio com a criança ou jovem vítima de cibercrime, crie todas as condições, nomeadamente através da **forma como comunica com a criança/jovem**, para que esta não sinta o momento do contacto ou do apoio como uma espécie "interrogatório policial", uma vez que não é, de todo, o que se pretende. É importante que o ambiente que seja confortável e informal, contribuindo-se para o estabelecimento de uma relação de confiança entre profissional e criança/jovem vítima.

Com crianças mais novas, o apoio pode implicar a presença de familiar ou representante legal, até a criança se habituar à presença do/a profissional e se sentir seguro/a sem a presença do/a familiar ou representante legal (APAV, 2019).

- **envolver, sempre que possível, a família**

3

O **papel da família e dos pais** é igualmente crucial no que respeita a situações de cibercrime ocorridas contra crianças e jovens. Assumindo o seu papel preventivo, devendo informar, supervisionar e, se for caso disso, restringir os comportamentos de utilização da Internet e das TIC por parte das

crianças e jovens (Öztürk & Akcan, 2016), o **envolvimento da família nas situações em que o cibercrime já teve lugar é igualmente importante**, já que:

- possuem um papel importante no relato da história de vida da criança ou jovem;
- a participação/frequência da criança ou jovem vítima no processo de apoio depende, em larga medida, da disponibilidade e disposição da família/pais;
- são elementos também chave para a psico-educação e prevenção da revitimação da criança ou jovem vítima.

O/A profissional deverá compreender em que medida a descoberta da experiência de cibervitimação da criança/jovem contribuiu para modificações no funcionamento e organização pessoal, conjugal e familiar. **A resolução do impacto e consequências da experiência de cibervitimação na família da criança/jovem vítima contribuirá também para a recuperação da própria criança**. As reações da família à experiência de cibervitimação das crianças e jovens são em tudo semelhantes às reações perante situações de violência e criminalidade *tradicional* (APAV, 2011):

- **Desejo de vingança**. Uma reação comum, associada a um sentimento de revolta, é o desejo de vingança, querendo fazer "justiça pelas próprias mãos";
- **Sentimento de culpa**. A família pode sentir-se culpada por não ter descoberto/suspeitado de que a criança ou jovem estava a ser alvo de crime ou violência;
- **"Assunto difícil"**. Falar com a criança ou jovem sobre a violência de que foi vítima é, geralmente, um desafio muito difícil para a família e para os pais. Ainda assim, este tipo de diálogos é importante para se estabelecer uma maior confiança na relação entre a família e a criança ou jovem. Pelo contrário, a família poderá tentar também pressionar a criança ou jovem a falar sobre a situação de vitimação, o que pode revelar-se contraproducente;
- **Mudança relacional**. Também a relação com a criança ou jovem pode alterar-se: a relação *família/pais-criança/jovem vítima* pode tornar-se mais difícil e turvada pelo constrangimento e por sentimentos recíprocos de culpa e vergonha;
- **Desconfiança em relação à intervenção**. O sentimento de falta de confiança manifesta-se, em muitos casos, em relação às instituições, designadamente às autoridades policiais. O facto de não lhes serem fornecidas informações sobre as investigações a decorrer é um elemento preponderante;
- **Afetação geral da vida**. Todas as áreas da vida pessoal, familiar, social e profissional dos elementos da família e dos pais podem ser afetadas;
- **Necessidade de apoio**. Complementarmente ao apoio e atuação junto da criança ou jovem vítima de cibercrime, a família e os pais poderão também necessitar de apoio específico, que os ajude o melhor possível nas tarefas e desafios acima indicados.

- **psico-educação para uma utilização segura e consciente das TIC e da Internet**

4

A atuação do/a profissional e da entidade em situações de cibervitimação de crianças e jovens deverá também preocupar-se, para além da resposta às necessidades precipitadas pela experiência de cibercrime, com a **promoção de comportamentos de utilização segura e consciente da Internet e das TIC**, tendo em vista a prevenção do envolvimento da criança ou jovem em novas situações de risco ou em situações de cibervitimação repetida.

É importante garantir que as crianças e jovens vítimas sejam educadas para uma utilização segura e adequada da Internet e das TIC, o que inclui, por exemplo: a adoção de comportamentos *online* adequados em matéria de proteção pessoal; a utilização positiva e segura das TIC e da Internet; a implementação de mecanismos de cibersegurança nas TIC e ferramentas de comunicação suportadas pela Internet; a identificação e atuação adequada perante situações de risco de cibervitimação (Martellozzo & Jane, 2017; Wolak, Finkelhor, Mitchell & Ybarra, 2010; Lwin, Ang & Liu, 2013; Wright, 2015).

DESTAQUE | PRÁTICAS EM FOCO:

No Reino Unido, o programa *ThinkUKnow* disponibiliza informações adaptadas a crianças de diferentes idades, bem como a famílias, pais, responsáveis legais e educadores/as sobre cibercrime e segurança *online*.

Este programa, criado pelo *Child Exploitation and Online Protection Centre* (CEOP), fornece conselhos e informações de segurança sobre uma série de questões relacionadas com a utilização da Internet e das TIC e situações de risco daí decorrentes (Marczak & Coyne, 2010).

A plataforma está disponível em: www.thinkuknow.co.uk/.

3. A PRESTAÇÃO DE APOIO A VÍTIMAS DE CIBERCRIME

Neste capítulo do Manual, e em estreita ligação com as orientações globais para o contacto, comunicação e recolha de informação abordadas no capítulo anterior, dedicar-nos-emos ao apoio e intervenção junto de vítimas de cibercrime.

Aludindo às consequências da experiência de cibervitimação e às necessidades de apoio que foram exploradas no capítulo 4 da parte I deste Manual, destacaremos o apoio emocional, bem como a intervenção em crise e os aspetos centrais do apoio especializado junto de vítimas de cibercrime.

Considerando a diversidade de formas de cibercriminalidade, importa destacar que o conteúdo ora apresentado não se propõe enquanto resposta única a implementar junto de qualquer vítima de cibercrime. Constitui, pelo contrário, um roteiro abrangente, contemplando linhas orientadoras de atuação que poderão auxiliar profissionais e entidades, com as devidas adaptações em funções das suas próprias características e objetivos, na definição e implementação dos seus procedimentos, tendo em vista a melhor resposta possível às necessidades das vítimas de cibercrime.

DESTAQUE | INFORMAÇÃO EM FOCO:

Muito embora este capítulo e os capítulos anteriores da parte *Proceder* deste Manual assumam, de antemão, que o apoio a vítimas de cibercrime seja assegurado por entidades, nomeadamente por organizações e estruturas de apoio à vítima, importa atender a alguns **requisitos-base e aspetos práticos para o desenvolvimento e operação de serviços de apoio para vítimas de cibercrime**.

Qualquer entidade que pretenda desenvolver e implementar um serviço ou resposta de apoio destinada a vítimas de cibercrime deverá considerar, primariamente, a realização de uma **avaliação diagnóstica das suas capacidades organizacionais**[99] para, de facto, desenvolver e operar um serviço ou resposta de apoio dessa natureza.

Algumas das dimensões que a entidade deve analisar internamente são as seguintes:

- Adequabilidade desse serviço ou resposta de apoio à missão e atividades da própria entidade e, quando aplicável, níveis de integração com os outros serviços já proporcionados pela entidade (nomeadamente, serviços e respostas de apoio para vítimas de crime e violência);
- Capacidade financeira para alavancar o desenvolvimento do serviço ou resposta de apoio e a sua operação, considerando, nomeadamente a (in)existência de recursos próprios, o acesso a financiamento externo e/ou a apoio mecenático;
- Acesso a recursos materiais, tecnológicos e logísticos necessários para desenvolver e operar o serviço ou resposta de apoio;
- Conhecimentos da entidade sobre o apoio a ser prestado e sobre a cibercriminalidade, incluindo sobre os diferentes tipos de cibercrime, os fatores de risco e o impacto da cibervitimação e o enquadramento legal aplicável;
- Capacidade técnica da entidade para desenvolver procedimentos de atuação para o serviço ou resposta apoio que pretende operar, considerando a sua adequabilidade à luz da missão, princípios e valores da própria entidade, das demais formas de apoio/serviços que disponibiliza e da legislação aplicável;
- Existência de parcerias (formais/informais) com entidades com experiência e conhecimento privilegiado neste domínio e possibilidade de participação/promoção de momentos de partilha/obtenção de

[99] Adaptado de Safety Net Project - https://www.techsafety.org/resources-agencyuse.

conhecimento, experiências e boas práticas;
- Existência de recursos humanos (remunerados e/ou voluntários/as) habilitados/as para prestar este tipo de apoio e capacidade técnica e financeira para a sua preparação e qualificação.

Assim, de forma sintética, a **preparação da entidade para a implementação** de uma resposta ou serviço de apoio para vítimas de cibercrime contemplará as seguintes etapas-base:

1. Definir os objetivos da resposta ou serviço de apoio que se pretende operar. Alguns dos objetivos podem ser, por exemplo: informação/sensibilização; apoio emocional; apoio prático; apoio ou aconselhamento mais específico a determinado nível (por exemplo, informação jurídica); encaminhamento para outros serviços/respostas/entidades adequadas ao tratamento da situação.
2. Identificar os/as destinatários/as da resposta ou serviço de apoio que se pretende operar: poderá pretender-se a implementação de uma resposta ou serviço de apoio que vise garantir o acesso a apoio e/ou a informação a vítimas de qualquer forma de cibercrime; poderá, no entanto, ser objetivo da referida resposta ou serviço orientar a sua intervenção para grupos específicos de vítimas e/ou para formas específicas de ciberciminalidade. Exemplo disso são as linhas de denúncia de material de abuso ou de exploração sexual de crianças.
3. Estabelecer procedimentos e estratégias de articulação e integração com as outras respostas e serviços de apoio para vítimas de crime que a entidade disponibiliza, caso estas existam, definindo como e de que forma a informação sobre uma determinada situação de cibervitimação será encaminhada internamente, caso seja necessário, para a melhor resposta às necessidades da vítima. Também deverá ser ponderada a articulação externa e a cooperação interinstitucional[100].
4. Desenvolver procedimentos específicos para o apoio que será prestado, considerando os objetivos e destinatários/as da resposta ou serviço de apoio, bem como a legislação aplicável[101] e códigos de conduta que orientam/regulam o exercício profissional, quando verificável, para além do conhecimento compreensivo sobre o fenómeno, sobre o seu impacto nas vítimas e sobre as necessidades precipitadas por experiências de cibervitimação[102].
5. Selecionar e formar recursos humanos para a operação da resposta ou serviço de apoio[103].
6. Divulgar e publicitar a resposta ou serviço de apoio[104].

3.1. Do apoio emocional à intervenção em crise

Sinteticamente, o apoio emocional a prestar junto de uma vítima de cibercrime assenta, em larga medida, na postura e atitude do/a profissional em torno de dimensões já abordadas neste Manual e que listamos em seguida:

- **Comunicação empática**, na qual se inclui a escuta ativa;
- **Linguagem não-verbal** do/a profissional demonstradora de disponibilidade, abertura e condizente com a escuta ativa;
- **Valorização da denúncia e respeito pelos ritmos** de partilha da vítima;
- Promoção da **expressão emocional da vítima e validação** da sua experiência e das reações, emoções/sentimentos, comportamentos, pensamentos e significados atribuídos a essa mesma experiência.

[100] Veja-se pontos 3.5.1.3. e 3.5.3.2. do capítulo 3 da parte II deste Manual, para informação adicional sobre o trabalho em cooperação.

[101] Veja-se capítulo 2 da parte I deste Manual, para informação detalhada sobre o enquadramento jurídico do cibercrime.

[102] Veja-se capítulos 1, 3 e 4 da parte I deste Manual, para informação compreensiva sobre o fenómeno da ciber-criminalidade, teorias explicativas, fatores de risco associados à cibervitimação e impacto do cibercrime.

[103] Veja-se capítulo 1 da parte II deste Manual, para informação sobre as competências pessoais e técnicas do/a profissional de apoio a vítimas de cibercrime.

[104] Veja-se ponto 4.2. da parte II deste Manual, para informação sobre o papel das campanhas públicas de informação e sensibilização na disseminação de informação sobre os recursos existentes para apoio e proteção a vítimas de cibercrime.

Nesse contexto, reforçamos, mais uma vez, que **este apoio emocional é especialmente importante aquando da recolha de informação** junto da vítima de crime relativamente à sua experiência de cibervitimação (até porque a recolha de informação, com a subsequente necessidade de partilha de informação sobre a experiência de cibervitimação, pode precipitar o surgimento de memórias e sentimentos negativos acerca da experiência de cibercrime; além disso, a recolha de informação é, em si mesmo, um momento desconfortável e de exposição para a vítima). Todavia, mantém-se como importante ao longo de toda a intervenção junto da vítima de cibercrime, independentemente de esta ser de natureza breve ou mais prolongada.

Porém, em determinadas circunstâncias, a vítima de cibercrime poderá procurar o apoio do/a profissional e da entidade na qual este/a exerce funções (nomeadamente as estruturas e organizações de apoio à vítima) em **situação de crise**.

DESTAQUE | INFORMAÇÃO EM FOCO:

A experiência de cibervitimação, pelo carácter potencialmente inusitado e surpreendente e pela ameaça (real ou percebida) à integridade física e/ou psicológica da vítima, poderá constituir um acontecimento potencialmente gerador de uma **situação de crise** (APAV, 2013).

A situação de crise é observável através das seguintes manifestações:

- **Reações psicológicas intensas**, tais como choro, pânico, confusão, angústia, vergonha, baixa autoestima, culpa, revolta, perturbações psicossomáticas[105] e predomínio de memórias sobre o evento;
- **Pressões sociais e económicas** que propiciam o bloqueio, associadas ao **desconhecimento dos seus direitos**.

A duração e intensidade da situação de crise depende do grau de violência exercida contra a vítima, dos seus recursos internos para enfrentar o problema e dos recursos externos que tem ao seu dispor, nomeadamente o apoio (informal e formal) recebido após a situação de vitimação.

A intervenção em crise (ou primeiros socorros psicológicos) constitui, por isso, uma atuação intensiva, focalizada e limitada no tempo, orientando-se para a resolução de problemas atuais e respondendo a objetivos específicos. Trata-se de uma resposta de apoio inicial, de cuidados práticos, não invasivos, em situações de crise ou emergência.

A tarefa inicial do/a profissional que contacta com uma vítima de cibercrime em situação de crise prende-se, por isso, com:

- A **avaliação da segurança da vítima** e da sua **capacidade de autocuidado** perante situações potencialmente traumáticas, considerando que os recursos pessoais e sociais de que dispõe podem ser insuficientes para responder adequadamente a uma situação de elevada exigência.
- Operacionalização de tarefas de intervenção orientadas para a **recuperação e reorganiza-**

[105] Perturbações psicossomáticas dizem, resumidamente, respeito à apresentação física (por exemplo, enjoos e dores de estômago) de problemas e desordens psicológicas.

ção da vítima, reduzindo o impacto negativo da cibervitimação e garantindo a sua segurança e o seu bem-estar físico e psicológico.

A intervenção em crise deve procurar responder aos seguintes objetivos, em tudo semelhantes às orientações gerais para o contacto com vítimas de cibercrime (veja-se Quadro 2):

- Romper com a ideia de caso único;
- Lidar com a procura de explicações;
- Lidar com sentimentos de culpa da vítima;
- Evitar o silenciamento ou a pressão "para esquecer";
- Promover a esperança na recuperação e resolução do problema;
- Explicar os procedimentos legais necessários.

A intervenção em crise deverá, por isso, pautar-se pelas seguintes **etapas**:

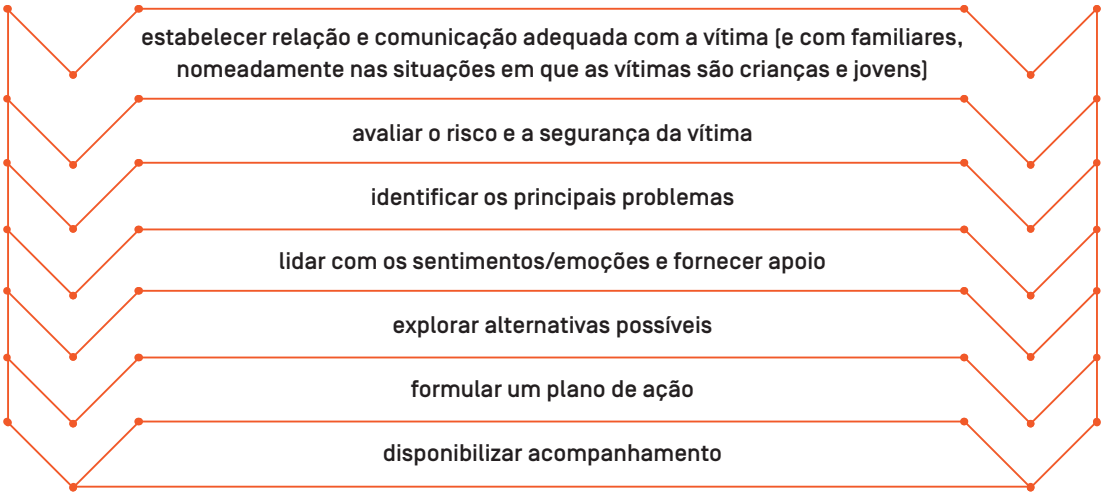

Figura II-2: Etapas da intervenção em crise

Neste tipo de intervenção sugere-se a adoção das seguintes estratégias, sem prejuízo de outras que podem ser entendidas como adequadas (APAV, 2013):

Estabelecer relação e comunicação com a vítima:
O/A profissional deve procurar estabelecer uma relação de confiança com a vítima, identificando os eventos que levaram à procura de apoio, o que permitirá identificar os problemas-chave.

Avaliar:
O/A profissional deve estar atento/a ao estado de saúde mental da vítima, nomeadamente, se existem ideações suicidas, qual o grau de ansiedade, de agitação e de angústia e, em particular, se a sua condição mental permite responder adequadamente às obrigações práticas decorrentes da cibervitimação.

O/A profissional deve também avaliar o risco (detalhes adicionais sobre esta matéria serão abordados nos pontos seguintes deste Manual), bem como a existência e qualidade do apoio proporcionado pela rede de suporte primária (família e/ou amigos/as).

Diminuir a ativação e a angústia:
É comum a vítima encontrar-se numa situação de ativação e de angústia. Comunicar com a vítima de uma forma segura e tranquilizante é uma estratégia adequada para reduzir estes sintomas. Identicamente, o momento/contacto com o/a profissional deverá ser utilizado com o propósito de explicar à vítima que as reações tidas são naturais, legítimas e podem ocorrer perante experiências pessoais negativas, desafiantes e/ou exigentes.

Neste processo, deverá comunicar-se de forma natural com a vítima (sem negligenciar a seriedade da situação vivida), prestando-lhe atenção e desencorajando comportamentos agitados ou emocionalmente ativados.

Mostrar interesse e encorajar:
O/A profissional deve demonstrar interesse, disponibilidade para escutar e compreender a vítima e sua situação (veja-se ponto 2.2. desta parte do Manual, no qual a empatia é explorada). Deve estimular ainda a esperança numa resolução positiva da situação (pese embora realista), o que promoverá a autoconfiança da vítima.

Importa também encorajar a vítima a encontrar as suas próprias estratégias para ultrapassar a experiência de cibervitimação, reforçando as suas capacidades.

Clarificar:
É importante clarificar quais são as exigências a que a vítima terá de fazer face na sequência do cibercrime de que foi alvo, incluindo obrigações práticas, como a articulação com entidades bancárias, em situações de cibercrime financeiramente motivado, por exemplo, ou a articulação com plataformas nos quais os conteúdos ilícitos estão disponíveis, tendo em vista a sua remoção.

Informar e validar os direitos da vítima:
O/a profissional deverá prestar à vítima informações sobre os seus direitos, sobre o funcionamento do sistema de justiça e sobre as vantagens e desvantagens da denúncia do crime, contribuindo-se, assim, para uma decisão informada da vítima nesta matéria. Uma das vantagens que podem ser associadas à decisão de denunciar poderá ser a tranquilização da vítima, pelo facto de assumir uma atitude ativa perante o crime de que foi vítima. Outra vantagem que poderá ser apontada pelo/a profissional prende-se com o facto de a vítima, através da denúncia da sua situação em concreto, estar a contribuir preventivamente para que outras pessoas possam ser "poupadas" de experienciar

situações de cibervitimação como a sua. As desvantagens prendem-se com as dificuldades que a vítima poderá vir a enfrentar ao longo do processo judicial, nomeadamente eventuais obstáculos na investigação criminal e as suas próprias dificuldades emocionais, tais como a vergonha sentida e a necessidade de reviver o acontecimento traumático, de cada vez que for solicitada a relatar os factos.

O/A profissional deverá alertar a vítima para a necessidade de preservar os meios de prova do crime, caso esta tenha acesso aos mesmos (como, por exemplo, *links* onde seja possível aceder a informação sobre os atos de agressão *online* a que tenha sido sujeita, bem como mensagens, vídeos e/ou outros ficheiros que tenha recebido durante a cibervitimação ou mesmo *prints*/cópias que dão conta da publicitação/divulgação da agressão *online*).

Encaminhar para autoridades judiciárias e policiais:
Caso a vítima, até ao momento do contacto com o/a profissional de apoio, não tenha contactado as autoridades judiciárias e policiais para a investigação destes crimes, poderá o/a profissional, com o consentimento da vítima, facilitar esse encaminhamento. Para o efeito, é importante que a entidade no qual o/a profissional exerce as suas funções de apoio defina e/ou procure implementar mecanismos facilitadores da cooperação interinstitucional, aspeto que abordaremos também neste Manual (veja-se ponto 3.5.1.3. e ponto 3.5.3.2. deste capítulo da parte II deste Manual).

Disponibilizar acompanhamento:
O/A profissional deverá colocar à disposição da vítima os serviços e respostas de apoio de que a entidade no qual exerce funções dispõe, o que pode incluir, por exemplo, o encaminhamento para serviços de apoio mais específicos proporcionados pela própria entidade e/ou serviços e mesmo recursos externos disponíveis, a nível local, regional ou nacional, através da articulação e cooperação interinstitucional.

DESTAQUE | PRÁTICAS EM FOCO:

A APAV coordena, em Portugal, uma rede especializada no apoio a crianças e jovens vítimas de violência sexual, denominada Rede CARE, que presta, de forma gratuita, apoio psicológico, social e jurídico a crianças e jovens vítimas de violência sexual, mas também a familiares e amigos/as.

Esta Rede conta com profissionais especializados/as, distribuídos pelo território, procurando assegurar um serviço de qualidade e proximidade. Através da atuação numa lógica de itinerância e mobilidade, os/as técnicos/as de apoio à vítima especialistas da Rede CARE garantem às crianças e jovens vítimas, seus familiares e amigos/as o acesso a apoio multidisciplinar, ajustado às necessidades identificadas e próximo das respetivas áreas de residência.
Assim, perante uma situação de violência sexual contra crianças e jovens que seja identificada em qualquer serviço de apoio de proximidade da APAV – como um Gabinete de Apoio à Vítima ou o Sistema Integrado de Apoio à Distância/Linha de Apoio à Vítima | 116 006 -, há lugar ao encaminhamento (interno) do caso para apoio especializado na Rede CARE.

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

Além da intervenção em crise, poderá ser necessária uma intervenção mais continuada junto da vítima de cibercrime, tendo em vista a reorganização e recuperação da vítima de cibercrime e a resposta adequada às suas necessidades. Em linha com as respostas de apoio disponibilizadas por outras estruturas e organizações de apoio à vítima para outras formas de vitimação, também este Manual abordará os aspetos centrais associados à intervenção especializada ao nível jurídico, psicológico e social, sendo estes domínios inclusivamente consonantes com as necessidades habitualmente identificadas nas/pelas vítimas de crime. Os aspetos-chave da intervenção especializada serão analisados no ponto 3.5. deste capítulo.

3.2. Avaliação do risco de revitimação

A avaliação do grau de risco de revitimação procura aferir a **probabilidade de ocorrência de novas situações de cibervitimação contra a vítima**. Com efeito, após a recolha de informação (veja-se capítulo 2 desta parte do Manual), deverá o/a profissional avaliar os fatores de risco e de proteção[106] evidenciados no caso alvo de intervenção, para que as necessidades de apoio e de intervenção possam ser identificadas.

O processo de avaliação do risco de revitimação resulta, assim, da convergência entre a **informação partilhada pela vítima** relativamente à sua experiência de cibervitimação e a utilização dessa mesma informação para **identificar (de forma mais ou menos estruturada) os fatores de risco de revitimação** presentes em cada caso em concreto (e que merecerão atenção particular, no que respeita à intervenção e planificação dos comportamentos de proteção pessoal *online* e de medidas de cibersegurança, tendo em vista a prevenção da revitimação). A **experiência e julgamento do/a profissional** de apoio é também importante neste processo de determinação do risco.

Figura II-3: Avaliação do risco de revitimação

[106] Para informação adicional sobre fatores de risco associados à cibervitimação, queira consultar capítulo 3 da parte I deste Manual.

3. A PRESTAÇÃO DE APOIO A VÍTIMAS DE CIBERCRIME

Como referido no capítulo 3 da parte I deste Manual, a investigação relativa aos fatores de risco associados à cibervitimação não é, até à data, especialmente extensa, sendo que, ainda que outros fatores ou variáveis possam vir a ser identificadas, os **fatores individuais relativos aos comportamentos da vítima**, nomeadamente a intensidade e os hábitos de utilização da Internet e das TIC e o tipo de atividades realizadas *online*, têm sido associados à maior vulnerabilidade ao cibercrime e ao risco de cibervitimação (Wilsem, 2013; Brown et al., 2017; van der Wagen & Pieters, 2018). Por outro lado, a multiplicidade de formas de cibercriminalidade dificulta também a identificação de um grupo de fatores ou variáveis de risco que sejam inequivocamente aplicáveis a qualquer tipo de cibercrime.

Ainda assim, mesmo que de forma genérica, poderemos dizer que a avaliação do risco de revitimação se deverá centrar em **3 domínios de risco**:

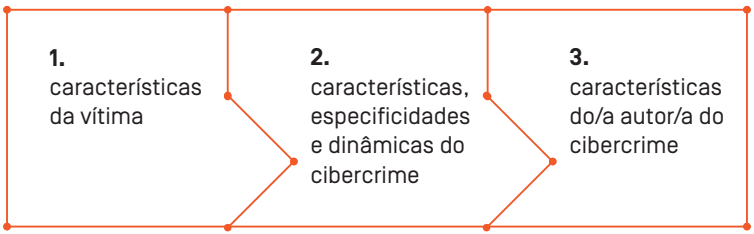

Figura II-4: Avaliação do risco de revitimação – áreas/domínios

No entanto, e aludindo, mais uma vez, à natureza múltipla da cibercriminalidade, torna-se claro que, por exemplo, a **análise do risco de revitimação por cibercrimes contra computadores e sistemas informáticos** (crimes ciber-dependentes)[107] dificilmente reúne informação que permita esta leitura tripartida do risco (assente nas características da vítima, nas dinâmicas do cibercrime e nas características do/a autor/a do cibercrime). Apenas a título exemplificativo, nestes casos, o/a autor/a do cibercrime atua de forma anónima, sendo muitíssimo difícil identificar a sua real identidade, pelo que a análise das suas características e do seu contributo para o aumento/redução do risco de revitimação é, desde logo, negativamente impactada.

Por outro lado, a identificação e a análise do risco a três níveis será mais útil para a determinação da vulnerabilidade da vítima à **revitimação nos casos de cibercriminalidade facilitada ou praticada por intermédio de computadores e sistemas informáticos**[108], nomeadamente nas situações em que existe algum tipo de nexo relacional (*online* e/ou *offline*) entre vítima e autor/a, já que estes casos mais facilmente correspondem a uma transposição da criminalidade *tradicional* para o ciberespaço.

Ainda assim, no quadro seguinte, apresentamos algumas variáveis e fatores de risco, associados a cada um dos domínios de risco supra, e que poderão ser considerados pelo/a profissional para a ponderação do risco de revitimação da vítima alvo de intervenção.

[107] Veja-se capítulo 1 da parte I deste Manual, para informação detalhada sobre esta concetualização.

[108] Idem.

É, contudo, relevante compreender que estas variáveis são indicativas e genéricas e não consideram as dinâmicas específicas associadas a cada situação particular de cibervitimação.

Quadro II-6: Proposta de variáveis para avaliação do risco de retivimação da vítima de cibercrime

Características da vítima	Características do cibercrime
Inclui fatores de risco relativos às características sociodemográficas e individuais da vítima e fatores de risco associados aos comportamentos de utilização da Internet e das TIC.	*Inclui características, especificidades e dinâmicas do cibercrime, incluindo a existência de algum tipo de relação/conhecimento (online e/ou offline) entre vítima e autor/a do cibercrime, nomeadamente nas situações de cibercriminalidade possibilitada ou facilitada pela Internet e pelas TIC.*
Idade *Têm sido evidenciados níveis diferenciados de risco de cibervitimação nas crianças/jovens e nas pessoas idosas; no primeiro caso, pelos hábitos de utilização intensiva da Internet e das TIC e, no segundo caso, pela falta de literacia tecnológica.* **Sexo** *A investigação e os estudos de prevalência não são consensuais, devendo esta variável ser interpretada com cautela. Embora o sexo feminino surja associado a níveis mais elevados de vitimação por diferentes cibercrimes, poderá dever-se à maior facilidade de revelação/denúncia da situação. O sexo masculino também surge associado, em alguns cibercrimes, a formas mais severas e graves de agressão.* **Outras variáveis individuais associadas à maior vulnerabilidade à vitimação** Presença de dificuldades mentais e/ou cognitivas/incapacidade *Estas características podem limitar ou dificultar a identificação/reconhecimento da cibervitimação e/ou a revelação/pedido de apoio, na sequência de cibervitimação, o que aumenta o risco de revitimação.* Língua nativa *Nas situações em que a língua nativa da vítima é diferente da língua onde o apoio/denúncia do cibercrime pode ser efetivado, o risco de revitimação é maior, associando-se também à maior vulnerabilidade à exclusão social e isolamento.* Experiências anteriores de vitimação *Caso a vítima tenha já sido alvo de cibercrime no passado, o risco de revitimação pode ser maior, considerando que podem manter-se inalterados os fatores de exposição ao cibercrime.* Inexistência de apoio informal (por exemplo, família; amigos/as; colegas de trabalho) *O isolamento social, nomeadamente face a relações sociais mais próximas e significativas, é fator de risco de vitimação.*	**Conhecimento relativamente ao/à autor/a do cibercrime** *O risco de revitimação é maior nas situações em que autor/a e vítima se conhecem (online e/ou offline). Nestes casos, o conhecimento das rotinas de vida da vítima, tanto online, como offline, é maior, o que aumenta risco de revitimação.* **Relacionamento com o/a autor/a do cibercrime** *Nas situações em que vítima e autor/a têm/tiveram algum tipo de relacionamento offline (como anteriores parceiros/as íntimos/as, colegas de trabalho, amigos/as), o risco de revitimação é maior.* **Existência de histórico de vitimação praticado pelo/a autor/a do cibercrime** *A existência de experiências anteriores de vitimação praticadas pelo/a mesmo autor/a constitui dinâmica indicativa de risco de revitimação. Um dos melhores preditores do comportamento atual do/a autor/a é o seu comportamento passado.* **Gravidade e impacto do cibercrime** *Por exemplo, o facto de o cibercrime poder ter desencadeado sintomas de desajuste emocional e psicológico (como ataques de pânico, medo intenso, flashbacks, pesadelos, tristeza profunda ou outros sintomas/sinais), poderá aumentar a redução da capacidade de procura de apoio perante atuais/futuras situações de vitimação.* **Duração e escalada do cibercrime** *Caso a cibervitimação seja continuada, como ocorre em muitas situações de ciber-stalking, por exemplo, para além de existir a probabilidade de as condutas ilícitas se tornarem mais intrusivas e agressivas para a vítima, reforçam/encorajam a conduta do/a autor/a, aumentando o risco para a vítima.* **Existência de medo relativamente ao/à autor/a do cibercrime** *A perceção de medo da vítima face ao/à autor/a do cibercrime, nomeadamente nos casos em que vítima e autor/a se conhecem, é um indicativo muito importante, pese embora existam situações de subestimação do risco.*

Fatores de risco associados aos comportamentos de utilização da Internet e das TIC

Literacia tecnológica
As competências e conhecimentos de utilização da Internet e das TIC parecem reduzir o risco de cibervitimação. Já a sua ausência/insuficiência, parece aumentar o risco de cibervitimação.

Níveis de utilização da Internet e das TIC
Pessoas com níveis mais elevados de utilização da Internet e das TIC [tempo de utilização diária, por exemplo] apresentam maior risco de cibervitimação.

Tipo de atividades realizadas online/conteúdos habitualmente consumidos
Índices mais elevados de desinibição nos comportamentos e interações online, bem como comportamentos de maior desproteção [como efetuar download de arquivos de origem não conhecida, por exemplo] estão associados à maior vulnerabilidade à cibervitimação.

Presença de tentativas anteriores [sem êxito] de resolução da situação
Para além do desânimo experienciado pela vítima, esse insucesso encoraja o/a autor/a na prática de novos atos contra a vítima, aumentando o risco.

Existência de denúncia
A denúncia é um momento de risco para a vítima, atendendo à possibilidade de retaliação/vingança por parte do/a autor/a.

Características do/a autor/a do cibercrime

Inclui características pessoais e sociais do/a autor/do cibercrime, as suas condutas prévias e outros indicadores de perigosidade que possam indiciar maior risco de revitimação para a vítima, nomeadamente nas situações de cibercriminalidade possibilitada ou facilitada pela Internet e pelas TIC.

NOTA: Neste domínio de análise do risco, além das dificuldades supra associadas às tipologias de cibercrime, a informação partilhada pela vítima poderá não ser suficiente para aferir os fatores abaixo apresentados.

Presença de **problemas de saúde mental e/ou consumo de drogas** pelo/a autor/a do cibercrime [de que a vítima tenha conhecimento]

Presença/histórico de **problemas com a justiça** por parte do/a autor/a do cibercrime [que a vítima tenha conhecimento]

Tentativas de **contacto/aproximação/intimidação** à vítima, depois do episódio que motivou a vítima a procurar apoio

Desejo de vingança por parte do/a autor/a, nomeadamente nas situações de cibercrime em que vítima e autor/a tiveram relação íntima anterior e cibercrime surge como forma de retaliação [por exemplo, divulgação não consensual de imagens e vídeos] face ao seu término

Particular interesse pelo cibercrime, por exemplo, por motivações financeiras e/ou pela procura de sensações

DESTAQUE | INFORMAÇÃO EM FOCO:

O/A profissional (e, neste caso, a entidade na qual exerce funções) deverão decidir e definir o modo como a recolha de informação para avaliação do risco de revitimação deverá ser efetuada. De forma genérica, poderemos considerar que:

- A recolha de informação pode ser realizada indiretamente pelo/a profissional, utilizando as informações partilhadas pela vítima aquando do contacto com a entidade/profissional;
- A avaliação do risco de revitimação poderá ser efetuada de forma mais estruturada, colocando questões concretas sobre cada uma das variáveis listadas acima (ou outras consideradas relevantes) e/ou através de instrumentos específicos.

- É importante lembrar ainda que a **avaliação do risco de revitimação só faz sentido se for acompanhada por medidas que possam ajudar a vítima a gerir e lidar com a situação e o risco em que se encontra**, com o propósito de aumentar a sua segurança e prevenir a revitimação.

Ao definir parâmetros e variáveis para avaliar o risco, a entidade e o/a profissional devem considerar também o desenvolvimento de informação e de um plano de segurança para a vítima, atendendo às variáveis de risco identificadas. O **plano de segurança** representa um conjunto de estratégias de prevenção da revitimação, acordadas e definidas entre vítima e profissional, no qual se inclui medidas e comportamentos de proteção face a novas situações de crime, bem como estratégias e instruções práticas para lidar e atuar, perante eventual re-ocorrência de cibervitimação.

O plano de segurança (Finn & Banach, 2000) poderá contemplar, consoante o tipo de cibercrime de que a vítima tenha sido alvo:

- A adoção de medidas de cibersegurança e comportamentos de proteção pessoal para a prevenção da revitimação, como, por exemplo: armazenar informações importantes em ficheiros e diretórios protegidos por palavra-passe; encriptar dados mais importantes; evitar fazer login e/ou partilhar informação pessoal a partir de redes públicas ou abertas de *wi-fi*; alterar *passwords*; atualizar *software* antivírus; modificar as definições de privacidade nas redes sociais;
- A identificação de sinais que possam indicar risco de cibervitimação, por exemplo: redirecionamento constante para páginas estranhas/não conhecidas da Internet; surgimento de mensagens de *pop-up*, imagens, sons estranhos ou aplicações instaladas sem consentimento, etc.;
- Informação prática sobre como e onde obter ajuda perante uma situação de vitimação.

3.3. Avaliação e identificação das necessidades de apoio

No seguimento da recolha de informação efetuada junto da vítima e considerando os resultados da avaliação do risco de revitimação, é importante que o/a profissional identifique as necessidades de apoio da vítima de cibercrime.

3. A PRESTAÇÃO DE APOIO A VÍTIMAS DE CIBERCRIME

Ora vejamos alguns aspetos que podem auxiliar o/a profissional na identificação das necessidades que carecem de atenção:

- Em que medida e de que forma(s) a vítima sente que foi afetada pelo crime/cibercrime de que foi alvo?
- De que forma está a experiência de cibervitimação a manifestar-se no funcionamento e bem-estar psicológico e emocional da vítima?
- De que forma está a experiência de cibervitimação a manifestar-se na saúde física da vítima?
- De que forma está a experiência de cibervitimação a manifestar-se no funcionamento relacional, laboral/ocupacional e social da vítima?
- De que forma está a experiência de cibervitimação a causar alterações na rotina e qualidade de vida (bem-estar geral) da vítima?
- De que forma está a experiência de cibervitimação a afetar a perceção pessoal de segurança e de cibersegurança (incluindo medo do crime)?
- Em que medida a experiência de cibervitimação afetou pessoas da sua rede social mais próxima e quais esses impactos?
- O que é a vítima deseja e necessita que aconteça após a experiência de cibervitimação?

Em função da resposta às linhas orientadoras anteriores, deverá o/a profissional, em conjunto com a vítima, apurar se:

- É necessário fornecer estratégias para aumentar a segurança da vítima para lidar com possíveis novos episódios de crime?
- É necessário recomendar que a vítima entre em contacto com as autoridades policiais/judiciárias?
- É necessário consciencializar a vítima para a necessidade de obter apoio, informações e/ou intervenções mais específicas (por exemplo, a nível jurídico, médico, psicológico ou outro)?
- É necessário sensibilizar a vítima para o encaminhamento para outros serviços ou entidades (por exemplo, para apoio médico/psiquiátrico específico).

DESTAQUE | PRÁTICAS EM FOCO:

No âmbito do Projeto EVVI (*EValuation of VIctims*), promovido pelo Ministério da Justiça Francês, foi desenvolvido um questionário de avaliação individual das necessidades das vítimas e um guia prático.

Este instrumento de avaliação das necessidades das vítimas encontra-se estruturado em diferentes domínios, nomeadamente:

- Características individuais da vítima e vulnerabilidade pessoal, como idade, sexo, etnia, presença de limitações ou dificuldades físicas e/ou cognitivas, entre outras;
- Risco e medo face ao crime, incluindo tipo e natureza do crime e as suas circunstâncias;
- Avaliação da situação atual da vítima;
- Histórico de vitimação e informação sobre o autor/a do crime.

O guia e o instrumento estão disponíveis em http://www.justice.gouv.fr/publication/evvi_guide_en.pdf.

Algumas das **necessidades identificadas** podem eventualmente ser respondidas pela própria entidade que se encontra a apoiar a vítima de cibercrime, nomeadamente através dos seus serviços e respostas de apoio.

No entanto, outras necessidades (por exemplo, apoio médico e psicoterapêutico) podem exigir a **cooperação interinstitucional e o envolvimento de outras estruturas**, por exemplo do sistema de justiça criminal e de outros sistemas. Aliás, a existência de parcerias intersectoriais, inclusivamente entre o Estado e as organizações da sociedade civil e de voluntariado, parecem ser importantes para a melhor resposta às necessidades das vítimas de cibercrime, na medida em que contribuem para amplificar a flexibilidade e acessibilidade a esses mesmos serviços e respostas de apoio (Wedlock & Tapley, 2016).

DESTAQUE | INFORMAÇÃO EM FOCO:

A capacidade de resposta da entidade às necessidades identificadas junto da vítima de cibercrime dependerá:

- das competências e missão da própria entidade;
- da existência/disponibilização de serviços ou respostas de apoio prestadas por parte da própria entidade e às quais o/a profissional possa recorrer para o encaminhamento da vítima de cibercrime para apoio específico/especializado em determinado domínio;
- existência de serviços ou respostas de apoio na comunidade (ao nível da Saúde, Segurança Social, Justiça e Segurança, por exemplo) e inclusive possíveis protocolos de cooperação interinstitucional[109].

3.4. O papel do apoio através da Internet no apoio a vítimas de cibercrime

Até este ponto do presente Manual, temos vindo a abordar o contacto e o apoio junto de vítimas de cibercrime, assumindo que estes decorrem através de modalidades convencionais (ou seja presencialmente e mesmo telefonicamente) de apoio, informação e intervenção. No entanto, do mesmo modo como a criminalidade e a violência foram transpondo barreiras físicas e convencionais e se consubstanciaram no surgimento do cibercrime e dos múltiplos fenómenos associados, também o contacto e o apoio a vítimas de crime têm vindo a evoluir.

São cada vez mais frequentes os serviços de apoio através da Internet disponibilizados por parte de organizações e estruturas de apoio à vítima para o apoio e informação junto de vítimas de crime.

Identicamente, também o apoio a vítimas de cibercrime poderá ser fornecido ou prestado através de serviços convencionais de apoio (nomeadamente de apoio presencial e de apoio telefónico), bem como por serviços de apoio através da Internet, entendendo-se estes últimos como canais igualmente válidos para o acesso ao mais variado tipo de serviços (Dooley et al., 2010).

[109] Veja-se pontos 3.5.1.3. e 3.5.3.2. deste capítulo da parte II do Manual, para informação sobre cooperação interinstitucional e trabalho em rede.

Importa, por isso mesmo, desconstruir alguns aspetos associados ao apoio através da Internet.

O **apoio através da Internet** constitui uma designação abrangente que diz respeito a todo o apoio, informação e/ou intervenção obtida remotamente, através da Internet e das TIC (Mallen, Vogel, Rochlen, & Day, 2005, Barak, Klein, & Proudfoot, 2009 *cit in* APAV, 2017).

Esta designação incorpora um conjunto diversificado de métodos, incluindo mecanismos de intervenção ou apoio em que pode ou não existir interação entre um/a utilizador/a e um/a profissional. Os diferentes métodos de apoio através da Internet podem divergir na (in)existência de interação com profissional, mas também no veículo utilizado para comunicar (por exemplo, áudio, vídeo e/ou texto), na complementaridade com outras formas de intervenção/apoio e na forma como a comunicação é efetuada (síncrona ou não síncrona) (Robinson, 2009, Callahan & Inckle, 2012 *cit in* idem).

São múltiplas as formas de apoio através da Internet, nomeadamente: programas de intervenção/apoio baseado na Internet; apoio *online*; blogues, fóruns e grupos *online* de ajuda mútua; *software* operado pela Internet; outras formas autoadministradas de apoio *online* (Barak et al., 2009, Dowling, & Rickwood, 2013 *cit in* idem).

De entre as diferentes formas de apoio através da Internet, destaque para o **apoio *online***, enquanto abordagem de apoio à distância que mais se assemelha às respostas tradicionais de apoio, informação e/ou intervenção presencial.

Por apoio *online* (APAV, 2019), entende-se a prestação de apoio e/ou informação a uma vítima de crime em que:

- A comunicação é efetuada utilizando a Internet e as TIC;
- O apoio e/ou informação são prestados remotamente (isto é, à distância), encontrando-se o/a profissional e a vítima em espaços físicos diferentes;
- A comunicação pode ser efetuada de forma síncrona (em tempo real, como é o caso dos serviços de *chat* e da comunicação através de aplicações como Skype® ou Whatsapp®) ou assíncrona (em que existe um hiato temporal entre a comunicação efetuada pela vítima e a resposta do/a profissional, como é o caso das mensagens de *e-mail* ou dos formulários *online*).

Pese embora a escassez de evidências relativamente à eficácia do apoio através da Internet e do apoio *online*, incluindo no que diz respeito à intervenção com vítimas de crime, são variadas as vantagens e benefícios apontados.

DESTAQUE | ESTATÍSTICAS EM FOCO:

No âmbito do *Projeto T@LK – online support for victims of crime*, promovido com o apoio financeiro do Programa Justiça da União Europeia, foi realizado um inquérito sobre apoio à distância e apoio *online* a vítimas de crime junto de 60 organizações e serviços de apoio à vítima da Europa. Entre outras matérias, este inquérito explorou as vantagens da prestação de apoio *online* a vítimas de crime:

- 82% das entidades participantes referiram a *acessibilidade* aos serviços de apoio como vantagem.
- Cerca de 80% das entidades participantes com apoio *online* apontaram a conveniência e a *flexibilidade* no acesso aos serviços de apoio como vantagens, sendo em menor dimensão (58%) as entidades sem serviços para a prestação de apoio *online* a vítimas de crime que indicaram a conveniência e flexibilidade enquanto aspetos positivos.
- O *acesso facilitado*, em particular para vítimas com dificuldades em aceder aos serviços de apoio convencionais, foi apontado como vantagem por 60% das entidades participantes com serviços de apoio *online* a vítimas de crime e por 74% das entidades participantes sem serviços de apoio *online*.
- A *facilitação de um primeiro contacto da vítima com os serviços e organizações de apoio* foi apontada como vantagem por 71% das entidades com apoio *online*, mas por apenas 42% das entidades sem serviços *online* para apoio a vítimas de crime.
- O *maior número de vítimas que pode ter acesso a apoio* foi apontado como vantagem por 79% das entidades participantes sem serviços de apoio *online*, mas em menor dimensão (57%) pelas entidades com serviços para apoio *online* a vítimas de crime.

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

DESTAQUE | PRÁTICAS EM FOCO:

- Ao abrigo do mesmo projeto, foi desenvolvido o *T@LK Handbook – online support for victims of crime*. Trata-se de um manual para estruturas e organizações de apoio à vítima, auxiliando-as na compreensão do apoio através da Internet, bem como na criação e/ou na implementação de serviços de apoio *online* para as vítimas de crime.

O manual pode ser acedido em https://www.apav.pt/publiproj/images/yootheme/PDF/Handbook_TALK.pdf.

3.5. O apoio especializado a vítimas de cibercrime

Na sequência da intervenção realizada, nomeadamente, se tiver sido caso, da intervenção em crise, e atendendo também à recolha de informação efetuada junto da vítima de cibercrime e à identificação das necessidades de apoio e proteção, poderá ser necessário o encaminhamento (interno ou externo) da vítima de cibercrime para respostas especializadas de apoio, nomeadamente a nível jurídico, psicológico e social, tendo em vista a minimização das consequências da cibervitimação, a reorganização da vida da vítima e a resposta às suas necessidades.

3.5.1. Apoio jurídico: objetivos e aspetos fundamentais

O apoio jurídico à vítima de cibercrime deve ser prestado exclusivamente por juristas, sendo, no entanto, de grande utilidade que qualquer profissional de apoio tenha conhecimento sobre o enquadramento jurídico nacional e demais instrumentos legais comunitários e internacionais que consubstanciam o regime jurídico aplicável. Recomenda-se, para o efeito, a leitura e consulta do capítulo 2 da parte I deste Manual, no qual é efetuado o enquadramento jurídico do cibercrime.

É ainda essencial que o/a profissional de apoio tenha presente as várias etapas do processo-crime e em que medida poderá informar e apoiar a vítima em cada uma das fases do processo e sobre os seus direitos enquanto vítima de crime.

O apoio jurídico compreende um conjunto de informações e diligências que permitem ao/à profissional acompanhar e apoiar a vítima de crime antes, ao longo e após as várias etapas do processo-crime.

O apoio jurídico consubstancia-se em:

- Informação sobre os tipos de cibercrime e seu enquadramento legal;
- Informação e aconselhamento sobre os direitos das vítimas de crime;
- Apoio na redação e apresentação de queixa/denúncia escrita;
- Apoio/acompanhamento pelo/a profissional de apoio na apresentação de queixa/denúncia;
- Apoio na redação de solicitação de aplicação de medida de proteção.
- Apoio na redação e apresentação de pedido de indemnização civil (quando a vítima o pode apresentar, sem ter para isso que constituir advogado/a);
- Apoio na análise de notificações judiciais e eventual redação de resposta;
- Apoio na redação de pedido de reembolso de despesas resultantes da participação no processo;
- Apoio na redação de requerimento para justificação de falta a diligência judicial;

3.5.1.1. Os direitos das vítimas de crime

Um ponto de partida essencial no apoio à vítima de crime é assegurar que, em qualquer fase do processo-crime, a vítima tem **acesso efetivo e exerce, de forma informada, os seus direitos**.

Aludindo à da transposição para os ordenamentos jurídicos nacionais dos Estados-Membros da União Europeia da Diretiva 2012/29/EU, do Parlamento Europeu e do Conselho de 25 de Outubro de 2012, que estabelece normas mínimas relativas aos direitos, apoio e proteção das vítimas da criminalidade, procura-se fortalecer a posição da vítima e as suas necessidades individuais de apoio e proteção no seu percurso pelo sistema de justiça penal, enfatizando o dever dos Estados em proteger as vítimas de crime, seus familiares e amigos/as face à vitimação secundária ou repetida, à intimidação e/ou à retaliação. Esta Diretiva vem ainda reforçar o papel essencial das organizações

de apoio à vítima, quer no seu papel complementar, ou em substituição do Estado, na garantia de acesso a serviços de apoio, qualificados, gratuitos e confidenciais, quer enquanto catalisadores de um exercício efetivo e informado dos direitos por parte das vítimas de crime.

Este Manual não dispensa a leitura integral da Diretiva[110], mas ressalva a importância do conhecimento completo dos vários direitos que este instrumento abriga.

Apresentamos, em seguida, uma síntese de alguns desses direitos, alertando, mais uma vez, para a importância da consulta e leitura integral do instrumento, bem como para a consulta de informação relativa à implementação prática desses mesmos direitos em http://www.infovictims.com/com/.

Direito à informação
O direito à informação é fundamental para que a vítima de crime possa participar de forma informada no processo-crime e exercer os seus direitos. A vítima de crime tem direito a receber, aquando do seu primeiro contacto com as forças de segurança ou autoridades judiciárias, informação sobre os seus direitos, nomeadamente:

- que tipos de apoio pode obter e quem os pode prestar;
- como e onde apresentar queixa ou denunciar um crime;
- como e em que circunstâncias pode requerer medidas de proteção;
- de que forma pode obter aconselhamento jurídico ou apoio judiciário;
- como e em que circunstância poderá requerer indemnização por parte do/a autor/a do crime;
- como e em que circunstâncias pode requerer indemnização do Estado;
- caso a vítima não domine a língua dos procedimentos ou seja portadora de deficiência, como pode beneficiar de serviços de interpretação e de tradução;
- caso não resida no Estado-Membro em que o crime ocorreu, que procedimentos existem para que possa exercer os seus direitos nesse país;
- caso as autoridades não respeitem os direitos da vítima, onde poderá esta dirigir-se para apresentar uma reclamação;
- quais os contactos que deve utilizar para obter ou acrescentar informação sobre o processo;
- quais os serviços de mediação disponíveis;
- como e em que circunstâncias pode requerer reembolso das despesas que resultem da sua participação no processo.

Direito a receber comprovativo de denúncia
Uma vítima que apresente denúncia ou queixa do crime sofrido junto da autoridade competente tem direito a receber um certificado de registo de denúncia ou queixa.

Direito a tradução
Quaisquer documentos e atos do processo-crime estão, em regra, na língua do país onde decorrem. É direito consagrado na Diretiva e, subsequentemente, de qualquer vítima em qualquer Estado-Mem-

[110] Documento completo da Directiva 2012/29/EU está disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32012L0029. A transposição para o ordenamento jurídico português foi efetuada pela Lei n.º 130/2015 (que introduziu as correspondentes alterações ao Código de Processo Penal e aprovou o Estatuto da Vítima).

bro, que esta possa participar de um ato do processo-crime, oralmente e/ou por escrito, numa língua que compreenda. Assim, deve a autoridade responsável pelo ato do processo-crime em causa, solicitar o apoio de intérprete ou tradutor que, simultaneamente, compreenda a língua dos procedimentos e a língua da vítima. Em função do papel assumido nos procedimentos, isto é, caso a vítima seja parte civil ou assistente no processo, tem direito a receber traduções, numa língua que domine, de toda a informação existente no processo e que seja essencial para o exercício dos seus direitos. Quando a vítima for portadora de deficiência, tem direito a receber interpretação numa forma que lhe permita uma efetiva participação nos procedimentos, i.e., requerer um intérprete de língua gestual ou requerer uma resposta por escrito a questões dirigidas oralmente.

Direito a acesso a serviços de apoio à vítima
A vítima tem direito a aceder a serviços de apoio à vítima, disponibilizados de forma gratuita e confidencial, ainda que tenha optado por não apresentar queixa formal ou denúncia do crime de que foi alvo.

Direito a ser ouvida
No decurso do processo-crime, a vítima tem direito a ser ouvida, disponibilizar informações importantes para a fase de inquérito e constituição de prova. Não obstante, deve a vítima, no momento de apresentação de queixa ou denúncia, disponibilizar o máximo de informação e elementos relevantes que permitam à autoridade responsável constituir prova. Ainda assim, está previsto que, no decurso da fase de investigação, a vítima possa acrescentar elementos adicionais quando intimada para prestar declarações junto do Ministério Público. Mais, caso o/a autor/a do crime venha a ser constituído/a arguido/a e o processo chegue a fase de julgamento, a vítima poderá acrescentar informações adicionais ou omissas até à data e a responder a questões colocadas pelos vários intervenientes no processo.

Há ainda a possibilidade de a vítima, em razão da sua particular vulnerabilidade, ser ouvida em sede de investigação ou instrução, sendo o seu depoimento gravado e utilizado em fases posteriores do processo-crime, evitando-se, deste modo, uma repetição do testemunho da vítima.

Direitos em caso de não acusação do/a arguido/a
Na eventualidade de, finda a fase de inquirição, o Ministério Público vier a considerar que não há prova suficiente para deduzir acusação e levar o/a arguido/a a julgamento, o processo-crime é arquivado. No cado de haver lugar à prática de vários crimes, pode o/a arguido/a vir a ser indiciado apenas relativamente a algum/alguns do(s) crime(s), sendo o processo arquivado para o(s) restante(s).

Nesta circunstância e caso a vítima discorde da decisão, tem direito a apresentar um requerimento ao/à juiz/juíza de instrução, solicitando a abertura de instrução. Pode ainda a vítima requerer a reapreciação de prova ou continuação da investigação, podendo, neste caso, apresentar nova(s) prova(s).

Direito a serviços de mediação
Em situações de pequena e média gravidade, como os crimes de ameaça, pequenos danos, agressões ou outros, a lei permite que o caso seja solucionado através de mediação entre vítima e argui-

do/a, caso este/a último/a tenha reconhecido a prática do crime.

O processo de mediação deverá ser gratuito, confidencial e voluntário, isto é, a vítima poderá optar ou não pela participação no mesmo a qualquer momento.

Este processo tem como finalidade proporcionar aos intervenientes um espaço de comunicação, com o apoio e facilitação de um interlocutor imparcial, para que a vítima possa transmitir qual o impacto e/ou o(s) dano(s) provocado(s) pelo crime e o/a arguido/a possa assumir responsabilidade pelo ato praticado.

O/A mediador/a é um/a profissional especificamente formado/a para o desempenho de mediação, sendo sua atribuição facilitar a comunicação entre os/as intervenientes.

Direito a informação ou proteção jurídica
O sistema de acesso ao direito e aos tribunais destina-se a assegurar que a ninguém seja dificultado ou impedido, em razão da sua condição cultural ou social, ou por insuficiência de meios económicos ou conhecimento, a usufruir do exercício e defesa dos seus direitos.

Assim, a vítima tem direito a consulta jurídica e aconselhamento sobre o seu papel em sede de processo-penal. Caso a vítima se constitua assistente ou seja parte civil, ou quando pretenda ser acompanhada por advogado/a e não disponha de meios financeiros para tal, tem direito a apoio judiciário, que pode consistir em: dispensa total ou parcial do pagamento da taxa de justiça; nomeação e pagamento de honorários de um/a advogado/a; pagamento faseado da taxa de justiça ou dos honorários do/a advogado/a.

Direito a compensação por participação no processo e a reembolso de despesas
Qualquer pessoa vítima que participe num processo-penal tem direito a ser compensado/a pelo tempo gasto com a sua participação, bem como a ser reembolsada/o pelas despesas daí decorrentes.

Direito à restituição de bens
Na eventualidade de quaisquer objetos ou demais bens da vítima sejam retidos pela(s) autoridade(s) competente(s), por constituírem meio de prova, e deixem de ser necessários para a boa condução do processo, estes devem ser restituídos sem demora. Esta restituição deve acontecer assim que possível, para que a vítima não fique privada dos seus bens para além do tempo estritamente necessário e imprescindível para as finalidades do processo-crime.

Direito a indemnização
Quem sofre danos resultantes da prática de um crime, tem o direito a ser indemnizado/a pelos mesmos.

O dever de indemnização recai sobre o/a autor/a do crime ou, em circunstâncias nas quais a prática do crime deixa a vítima em dificuldades económicas ou não permite que a vítima seja indemnizada em tempo útil pelo/a autor/a do crime, pode ser requerido ao Estado um pedido de adiantamento desta indemnização.

Direito a proteção
As vítimas e seus familiares têm direito a proteção contra atos de retaliação, de intimidação ou de continuação de atividade criminosa contra si. Têm direito a ser protegidas de atos que possam colocar em causa a sua vida, integridade física, bem-estar emocional e psicológico e a sua dignidade aquando da prestação de depoimento.

Sempre que as autoridades considerem que existe uma ameaça séria de atos de vingança ou fortes indícios de que a segurança e a privacidade da vítima podem ser grave e intencionalmente perturbadas, deve ser assegurado a esta, bem como à sua família ou outras pessoas próximas, um nível adequado de proteção.

A proteção e segurança das vítimas podem ser acauteladas através da aplicação ao arguido de uma ou mais medidas de coação, enquanto restrições à liberdade do arguido, que podem ser aplicadas no decurso do processo-crime, caso se verifique perigo de fuga, perigo para a obtenção e conservação da prova do crime, perigo para a ordem pública e/ou perigo de continuação da atividade criminosa.

Sempre que a vida da vítima ou de outra testemunha, a sua integridade física ou psíquica, a sua liberdade ou bens patrimoniais seus de valor consideravelmente elevado sejam postos em perigo por causa do seu contributo para a investigação e prova do crime, aquelas podem requerer a aplicação de meios de proteção.

Direitos das vítimas com necessidades especiais de proteção
Considera-se vítima com necessidades especiais de proteção aquela que, em função das suas características pessoais, do tipo ou natureza do crime sofrido e/ou das circunstâncias em que este ocorreu, está particularmente vulnerável à continuação da vitimação, à vitimação secundária, à intimidação ou à retaliação, pelo que necessita de cuidados especiais, sobretudo ao nível da proteção.

Esta vulnerabilidade deve ser avaliada caso a caso, mas deve ser dada particular atenção a vítimas que sofreram um dano considerável devido à severidade e gravidade do crime, a vítimas de crimes motivados por discriminação baseada em características pessoais e a vítimas cujo relacionamento e dependência face ao/à autor/a do crime as torne particularmente vulneráveis.

Consequentemente, merecem cuidado especial as vítimas de terrorismo, de crime organizado, de tráfico de pessoas, de violência de género, de violência no âmbito de relações de intimidade, de violência sexual e de crimes de ódio. Independentemente do tipo de crime sofrido, as crianças, as pessoas idosas e as pessoas debilitadas por doença ou portadoras de deficiência devem ser particularmente consideradas, aquando da avaliação da especial vulnerabilidade.

Direito a ser esquecido[111]
Este direito fornece ao seu titular a possibilidade de solicitar, verbalmente ou por escrito, que o/a responsável pelo tratamento de dados apague os seus dados pessoais. Este direito pode ser exercido sempre que a informação pessoal seja considerada inadequada, irrelevante ou que tenha perdido a sua relevância.

[111] Este direito, ao contrário dos anteriores, não integra a Diretiva 2012/29/EU. Consta no artigo 17.º do Regulamento Geral de Proteção de Dados Pessoais. Para informação adicional, veja-se ponto 2.2 do capítulo 2 da parte I deste Manual.

3.5.1.2. A importância da preservação da prova digital

"As provas têm por função a demonstração da realidade dos factos" (artigo 341.º do Código Civil) sendo que *"constituem objeto da prova todos os factos juridicamente relevantes para a existência ou inexistência do crime, a punibilidade ou não punibilidade do arguido e a determinação da pena ou da medida de segurança aplicáveis"* e havendo lugar a pedido civil, constituem objeto da prova os factos relevantes para determinação da responsabilidade civil (artigo 124.º n.ºs 1 e 2 do CPP). No que respeita ao princípio da legalidade da prova, no nosso ordenamento jurídico, o artigo 125º do Código de Processo Penal consagra que *"são admissíveis as provas que não forem proibidas por lei"*.

Por se tratarem de crimes que ocorrem no mundo digital, são diversos os obstáculos na sua investigação (Martellozzo & Jane, 2017). Os estudos e investigadores/as que se têm dedicado à análise da cibercriminalidade e das **dificuldades apontadas à denúncia[112] e investigação do cibercrime** têm indicado, entre outros, os seguintes obstáculos:

- o "local" onde a conduta criminal teve lugar;
- a identificação do/a autor/a do crime (especialmente devido ao anonimato proporcionado pelo ecossistema do ciberespaço e à impermanência e volatilidade de evidências e provas dos seus comportamentos, podendo estas ser facilmente bloqueadas, modificadas, inutilizadas ou apagadas);
- o estabelecimento de causalidade em casos que frequentemente envolvem múltiplos e difusos autores/as e vítimas.

Por outras palavras, estas dificuldades na investigação, evidenciam-se, por se tratar de um tipo de criminalidade que é transnacional, anónima e variável (em constante evolução e com novas formas de atuação em permanente surgimento) (Santos, 2016; Holt & Bossler, 2015).

DESTAQUE | PRÁTICAS EM FOCO:

O Projeto *SIRIUS*, liderado pelo *Europol's European Counter-Terrorism Centre* e pelo *European Cybercrime Centre*, em parceria com *Eurojust* e *European Judicial Network*, tem como objetivo auxiliar as autoridades a lidar com a complexidade e o volume de informações num ambiente *online* em rápida mudança.

Este projeto visa a partilha de conhecimento através de eventos, bem como por intermédio de uma plataforma restrita, na qual os Estados-Membros (e países terceiros com acordo operacional com a EUROPOL) podem encontrar informações atualizadas e acesso a provas digitais para investigação criminal.

Informação adicional está disponível em: www.europol.europa.eu/sirius.

No que respeita aos meios de prova, o uso das TIC em atividades criminosas popularizou a prova digital (Balkin et al., 2007).

[112] Veja-se, para o efeito, o ponto 1.4. da parte I deste Manual, em que são abordadas as cifras negras associadas à cibercriminalidade e os fundamentos para a não denúncia de situações de cibercrime.

Efetivamente, uma das diferenças mais significativas entre a cibercriminalidade e os crimes *tradicionais* diz respeito à natureza das evidências e da prova. Existem diferenças na forma que assumem, no modo como são armazenadas, onde estão localizadas e como podem ser encontradas. Além disso, a prova digital é intangível, geralmente volátil, podendo ser também massiva em quantidade, o que coloca desafios logísticos substanciais (Grabosky, 2007).

Assumindo a prova digital carácter temporário e de grande volatilidade, existem desafios adicionais para salvaguardar as demais características necessárias para ser válida, tornando-se imprescindível assegurar a sua admissibilidade, autenticidade, precisão e completude (Marques, 2013). A título exemplificativo, uma simples não conformidade no armazenamento da prova e a consequente quebra da cadeia da prova, provoca a sua anulação por inadmissibilidade legal (*idem*).

A prova digital, tal como os outros tipos de provas, deve ser manipulada, de modo a preservar o seu valor probatório, que se prende não apenas com a sua integridade física, mas sobretudo com os dados que ela contém. Dependendo do tipo de dispositivo, devem ser implementadas medidas especiais de recolha, acondicionamento, transporte e armazenamento (*idem*).

3.5.1.3. O papel da cooperação interinstitucional

Considerando a natureza da intervenção com vítimas de cibercrime e a resposta às necessidades de apoio identificadas, muitas vezes associadas com o processo-crime, é primordial considerar a importância da **articulação interinstitucional entre as organizações e serviços de apoio à vítima e as autoridades policiais e judiciárias**.

Idealmente, esses processos colaborativos interinstitucionais poderão ser operacionalizados, através da formalização de parcerias, por intermédio de **protocolos e acordos de cooperação**, que possibilitem a definição conjunta de procedimentos e a colaboração, tendo em vista a agilização de mecanismos de comunicação e de partilha de informação que contribuem para o melhor apoio, tratamento e intervenção proporcionados às vítimas de crime em geral e, em particular, às vítimas de cibercrime.

DESTAQUE | PRÁTICAS EM FOCO:

A Associação Portuguesa de Apoio à Vítima (APAV) e a Polícia Judiciária, autoridade que, em Portugal, tem competência reservada na investigação de cibercriminalidade, celebraram, em 2019, protocolo de cooperação, tendo em vista a colaboração no âmbito da Linha Internet Segura.

A Linha Internet Segura, operada pela APAV, ao abrigo do consórcio Centro Internet Segura, é um serviço de apoio telefónico e de apoio *online* com duas vertentes: o aconselhamento e informação em questões relacionadas com a utilização da Internet e das TIC, bem como o apoio e informação em situações de cibercrime (Helpline); a denúncia de conteúdos ilegais na Internet (Hotline).

Para além deste protocolo de cooperação prever o estabelecimento de um sistema de referenciação para a APAV de vítimas de cibercrime atendidas pela Polícia Judiciária, permite a transmissão eficiente de informação, no que respeita ao encaminhamento de denúncias de cibercrimes recebidas pelos serviços da Linha Internet Segura para a Polícia Judiciária.

Por norma, e como o exemplo acima partilhado confirma, estes protocolos e acordos proporcionam a possibilidade de serem definidos e implementados **mecanismos de encaminhamento e referenciação de vítimas de crime**.

Diga-se, a esse respeito, que a já referida Diretiva 2012/29/EU aponta precisamente a facilitação do encaminhamento das vítimas de crime pelas autoridades competentes para os serviços de apoio às vítimas, como forma de garantir o **direito da vítima em aceder a serviços de apoio antes, durante e por um período adequado após a conclusão do processo penal**.

Nesse seguimento e evolutivamente, poderemos apontar a **referenciação**, enquanto **mecanismo de articulação interinstitucional** no âmbito do qual uma entidade transmite a outra informações sobre a ocorrência de crimes e respetivas vítimas, com o consentimento destas e com a finalidade de lhes ser prestado apoio. A referenciação distingue-se do encaminhamento, porque assenta em processos pró-ativos e são parte integrante dos procedimentos de apoio a vítimas de crime de um determinado serviço ou organização de apoio. A referenciação implica sempre o respeito da vontade da vítima e o seu consentimento, promovendo-se o acesso da vítima de crime a um apoio mais especializado ou específico, que melhor responderá a necessidades previamente identificadas.

DESTAQUE | INFORMAÇÃO EM FOCO:

A forma de recolha e de transmissão de informação, com vista à referenciação das vítimas de crime, deve também ser estabelecida e acordada entre as entidades envolvidas num determinado mecanismo de referenciação.

Independentemente do(s) método(s) de recolha e de transmissão de informação, é fundamental que a informação transmitida contemple aspetos centrais que permitam identificar a vítima e compreender a situação de vitimação experienciada, minimizando o risco de ter que relatar novamente o(s) episódio(s) que motivaram o contacto com o serviço ou organização de apoio.

A seguinte informação-base deverá, por isso, ser incluída em qualquer processo de referenciação:

- Nome da vítima;
- Contacto da vítima e horário preferencial para contacto;
- Breve descrição do crime/situação de vitimação (tipo de crime; relação com o/a autor/a do crime, quando aplicável; consequências e impacto da vitimação);
- Observações e os apoios prestados pela entidade (ex.: apoio psicológico, informação jurídica e outras observações relevantes para o trabalho da entidade para a qual a vitima foi encaminhada).

DESTAQUE | PRÁTICAS EM FOCO:

O Projeto *VICToRIIA - Best Practices in Victims Support: Referrals, Information, Individual Assessment*, promovido pelo Centre for Crime Prevention in Lithuania (NPLC), com o apoio financeiro do Programa Justiça da União Europeia, visou, entre outras atividades e objetivos, o desenvolvimento de mecanismos de referenciação entre organizações de apoio à vítima e autoridades policiais. Entre as suas atividades, destacou-se o desenvolvimento de um manual - *Manual of effective and secure referrals of victims*.

Com diferentes recomendações para a definição e implementação de sistemas de referenciação eficazes e seguros para as vítimas de crime, o Manual destaca a importância da preservação da segurança da vítima, bem como a garantia de proteção dos seus dados pessoais, em linha com regulamento geral de proteção de dados pessoais (RGPD) e demais leis nacionais aplicáveis.

Informação adicional disponível em http://nplc.lt/victoriia/.

3.5.2. Apoio psicológico: objetivos e aspetos fundamentais

O apoio psicológico procura proporcionar uma experiência terapêutica à vítima e/ou à família e tem como propósito a minimização dos efeitos negativos da exposição a uma experiência adversa e potencialmente traumática. Responde, assim, à necessidade identificada na vítima e/ou nos seus familiares de restabelecimento do funcionamento e bem-estar psicológico e emocional comprometidos como resultado da experiência de vitimação (APAV, 2013).

O apoio psicológico deverá ser exclusivamente implementado por profissionais com habilitação supe-

rior em Psicologia e cujas habilitações e experiência tenham sido devidamente reconhecidas, quando aplicável, pela respetiva entidade que, no país em apreço, regula o acesso e o exercício da profissão.

São vários os modelos e as escolas utilizadas na intervenção psicológica junto de vítimas de crime, incluindo terapias da orientação psicodinâmica, intervenções cognitivo-comportamentais e terapias narrativas e construtivistas. Independentemente da abordagem teórica preferencial do/a profissional de apoio e/ou da entidade no qual exerce funções, é fundamental o conhecimento sobre as diferentes formas de cibercrime e suas dinâmicas, bem como sobre os fatores de risco associados à cibervitimação e ao seu impacto no funcionamento psicológico, emocional e social da vítima[113].

Apresentam-se como principais objetivos do apoio psicológico:

- Alívio e melhoria dos sintomas;
- Redução do desconforto e de comportamentos disfuncionais;
- Reforço dos mecanismos de defesa adaptativos;
- Melhoria da sua adaptação ao meio;
- Melhoria das capacidades de julgamento da realidade;
- Reforço da autoestima;
- Maximização da autonomia;
- Restabelecimento do equilíbrio psicológico.

Com efeito, nos pontos seguintes deste Manual, apresentamos linhas orientadoras e alguns dos aspetos-chave a considerar, necessariamente genéricos, para a implementação de respostas de apoio psicológico a vítimas de cibercrime. O conteúdo ora explorado não representa, portanto, um referencial ou um programa de intervenção psicológica com vítimas de cibercrime, mas, ademais, propõe pressupostos e princípios que devem ser atendidos em qualquer processo de intervenção desta natureza, independentemente da abordagem teórica utilizada e da entidade na qual tal intervenção seja operacionalizada.

3.5.2.1. Pressupostos e princípios operativos do apoio psicológico

Alguns dos **pressupostos** que devem ser considerados para o sucesso da intervenção psicológica com a vítima são (APAV, 2013; Alexy et al., 2005):

- O/A profissional deve estabelecer com a vítima uma aliança terapêutica e uma relação de suporte, não estigmatizante e não preconceituosa;
- O/A profissional deve avaliar adequadamente o impacto da experiência de cibervitimação, nomeadamente os indicadores de desajustamento psicológico, emocional e comportamental, incluindo o evitamento e a reexperienciação (sintomas associados ao pós-stress traumático), o funcionamento social e comportamento profissional, bem como o risco de suicídio;
- O/A profissional deve ainda avaliar possíveis comorbilidades[114] com outras perturbações ou

[113] Veja-se, para o efeito, os capítulos 1, 3 e 4 da parte I deste Manual, nos quais são explorados, respetivamente, as tipologias e os diferentes tipos de cibercrime, os fatores de risco sociodemográficos e fatores de risco comportamentais associados à experiência de cibervitimação e as consequências da cibervitimação.

[114] Comorbilidade ocorre quando duas ou mais perturbações se apresentam concomitantemente na mesma pessoa.

desordens mentais, encaminhando para outros profissionais e/ou serviços específicos mais especializados, se necessário;
- O questionamento deve ser oportuno e sensível, facilitando o discurso da vítima;
- O/A profissional deve validar os sentimentos, pensamentos e a história de vitimação relatada pela vítima;
- O/A profissional deverá ajudar a vítima a lidar com emoções e sentimentos adversos associados à experiência de cibervitimação, tais como o medo, a raiva, a culpa e a vergonha;
- O/a profissional deverá providenciar informação acerca das possíveis reações à experiência de cibervitimação, sendo capaz de enquadrar os referidos pensamentos, sentimentos e comportamentos eventualmente experienciados/tidos pela vítima enquanto reações e consequências naturais perante acontecimentos de vida inesperados, promovendo expectativas positivas quanto ao processo de recuperação;
- O/A profissional deve ajudar a vítima a encontrar estratégias que diminuam os evitamentos cognitivos e comportamentais e a lidar eficazmente com a possibilidade de revivência do acontecimento e da ocorrência de pensamentos intrusivos, como sentimentos de ineficácia, incompetência e desesperança, bem como de raiva, culpa e vergonha, promovendo o aumento da autoestima e o estabelecimento de relações de confiança.

Deverá ter-se ainda em consideração os seguintes **princípios operativos** (APAV, 2011; APAV, 2013):

Contrato terapêutico
No início do processo de apoio, deverá estabelecer-se com a vítima um conjunto de regras e procedimentos - o *contrato terapêutico*, definindo-se o horário, a frequência e a duração das sessões, as regras de assiduidade e da pontualidade, bem como apresentando-se os objetivos e o planeamento para a intervenção. Este contrato visa também comprometer e responsabilizar a vítima relativamente ao processo de apoio psicológico e aos sucessos daí provenientes, contribuindo para o envolvimento e adesão da vítima aos objetivos estipulados para a intervenção.

Neutralidade e anonimato
O/a profissional deverá comunicar e interagir com a vítima sem acrescentar opiniões pessoais, autorrevelações, manipulações e outras respostas desenquadradas do apoio psicológico. Pelo contrário, deverá promover a livre expressão emocional e afetiva da vítima, sem constrangimentos. Neutralidade não significa falta de empatia, sendo esta competência muito importante, como já foi abordado[115], para a construção de uma relação de confiança entre vítima e profissional de apoio.

Privacidade e sigilo
Deve ser garantido à vítima que as informações partilhadas no âmbito do apoio psicológico serão sempre mantidas dentro do escopo da intervenção. A transmissão de informação a terceiros (pessoas ou entidades) sobre o apoio psicológico, só decorrerá na sequência do consentimento prévio fornecido pela vítima para o efeito.

[115] Para informação adicional sobre a comunicação e empatia no contacto com vítimas de crime e de cibercrime, queira consultar o capítulo 2 desta parte do Manual.

3.5.2.2. Fases do processo de apoio psicológico

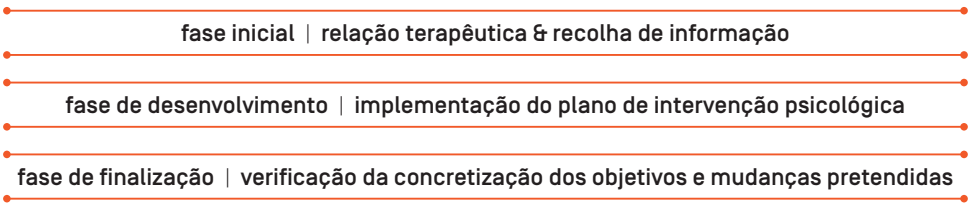

Figura II- 5: Fases do processo de apoio psicológico

Fase inicial do processo de apoio psicológico

Esta fase destina-se ao **estabelecimento de relação de confiança** entre a vítima e o/a profissional de apoio responsável pela intervenção psicológica. Para o efeito, são fundamentais as competências pessoais e técnicas do/a profissional, bem como a comunicação empática (veja-se pontos 2.1 e 2.2. do capítulo 2 da parte I deste Manual). É neste momento do processo de apoio que se estabelece o contrato terapêutico.

Na fase inicial deste processo de intervenção, deverá ter lugar a **recolha de informação** e sua análise, tendo em vista a definição de um plano e de estratégias de intervenção psicológica.

A este respeito, a recolha de informação realizada junto da vítima de cibercrime[116] por parte de (eventualmente) outros profissionais de apoio, em contactos prévios efetuados com a entidade, poderá ser útil, já que possibilita uma compreensão global da história de vida da vítima, dos seus recursos internos e externos, bem como da experiência de cibervitimação e dos seus impactos.

Adicionalmente, poderá recorrer-se a **guiões e entrevistas para recolha de informação e instrumentos de avaliação psicológica**, tendo em vista, respetivamente, o registo e sistematização de informação relevante para a definição da intervenção (nomeadamente o pedido e as necessidades da vítima no domínio emocional e psicológico) e a análise específica de domínios concretos do (dis) funcionamento psicológico e emocional. A recolha de informação junto da vítima deverá ser ainda complementada pela observação do seu comportamento e da sua **comunicação e linguagem não-verbal**, uma vez que daí decorrem indicadores importantes relativamente ao estado emocional da vítima e ao seu bem-estar e funcionamento.

A recolha de informação para a definição da intervenção psicológica poderá constituir, em si mesmo, um processo terapêutico, uma vez que, ao mesmo tempo que permite mapear os recursos (internos e externos) impactados pela experiência de cibervitimação, contribui para a livre expressão emocional da vítima e para o desenvolvimento de uma narrativa em torno da experiência de cibervitimação da qual foi alvo.

[116] Informação adicional sobre a importância da recolha de informação, está disponível no ponto 2.3. do capítulo 2 da parte II deste Manual.

Fase de desenvolvimento do processo de apoio psicológico

Esta fase é marcada pela **implementação do plano e das estratégias de intervenção psicológicas** definidas anteriormente, podendo decorrer ao longo de vários momentos ou sessões de intervenção. Prossegue-se ainda com a recolha e análise de informação, enquanto processo circular e transversal à intervenção a realizar.

Independentemente das estratégias de intervenção e da orientação/escola teórica utilizada, na implementação do plano de intervenção psicológica, deverá o/a profissional de apoio procurar:

- **Facilitar a expressão emocional e a comunicação**: o/a profissional deverá estimular a vítima a partilhar os seus sentimentos, emoções e pensamentos, assegurando-lhe e demonstrando-lhe que esta expressão será aceite sem julgamentos de qualquer tipo;
- **Promover na vítima uma compreensão dos seus problemas e das respostas**: o/a profissional deve elucidar a vítima quanto à natureza do crime de que foi alvo e apresentar-lhe situações de cibervitimação semelhantes à sua, facilitando a identificação com a sua própria história de vitimação e, subsequentemente, com as necessidades e problemas associados e possíveis soluções;
- **Mostrar interesse e empatia**: nesta matéria, veja-se pontos 2.1 e 2.2. do capítulo 2 da parte II deste Manual;
- **Fortalecer a autoestima**: o fortalecimento da autoestima da vítima contribui para a promoção das mudanças de comportamento que se pretendem com a intervenção psicológica;
- **Facilitar a resolução de problemas**: o/a profissional deverá auxiliar a vítima a enfrentar as dificuldades, a tomar decisões e a resolver os problemas, mediante a orientação para as soluções.

Fase de finalização do processo de apoio psicológico

Sendo difícil de determinar o momento adequado para a finalização do processo de apoio psicológico, deverá o/a profissional, para o efeito, rever os objetivos do plano de intervenção inicialmente desenvolvido, percorrendo-os com a vítima para:

- Averiguar o significado que esta atribui à sua experiência de cibervitimação e em que medida considera que os objetivos estabelecidos estão total ou parcialmente alcançados;
- Antecipar estratégias de prevenção e proteção;
- Confirmar as competências adquiridas para manter as melhorias e mudanças alcançadas com o processo de intervenção.

Após a finalização, é importante o/a profissional proceder ao **seguimento/follow-up** do caso, para recolher informação sobre a manutenção dos resultados obtidos após o termo do apoio psicológico.

Independentemente do momento ou fase do processo de apoio psicológico, o quadro seguinte apresenta algumas técnicas de comunicação que podem auxiliar a prossecução dos objetivos definidos para a intervenção (APAV, 2013).

Quadro II-7: Técnicas e estratégias de comunicação úteis para o processo de apoio psicológico

Catarse - facilitar a expressão de sentimentos e emoções

Questionamento - realizar perguntas fechadas (ex.: "Como se chama?") ou abertas (ex.: "O que pensa sobre isso?") para a obtenção de informação

Reestruturação - reorganizar a informação partilhada pela vítima de uma outra forma, permitindo uma mudança de perspetiva sobre o tema

Focagem - selecionar, de entre a informação partilhada pela vítima, a que parece mais relevante para determinado objetivo da intervenção

Interpretação - acrescentar sentido a algo que foi expresso pela vítima

Clarificação - tornar mais claro o foi dito pela vítima, para maior compreensão acerca dos seus sintomas, afetos e comportamentos

Confrontação - comparar conteúdos discrepantes sobre o mesmo tema, para esclarecer dúvidas, devolver incongruências e/ou desafiar verbalizações ou comportamentos da vítima

Sugestão - Induzir uma ideia ou sentimento para sugerir cenários alternativos

Ecoar – repetir palavra ou interrogação sobre alguma informação partilhada pela vítima, como forma de manter a atenção da vítima face ao processo de intervenção e reforçar a comunicação empática e a relação entre profissional e vítima

Silêncio - serve sobretudo para possibilitar espaço à reflexão

Securização - tranquilizar e reforçar a autoestima da vítima, através da expressão de concordância com uma ideia, pensamento, atitude ou decisão

Aconselhamento - apresentar atitudes ou decisões, com vista a reforçar aspetos saudáveis da conduta da vítima, reduzir sintomas ou evitar crises

Educação - Esclarecer a vítima sobre assuntos ou situações relevantes

3.5.3. Apoio social: objetivos e aspetos fundamentais

Por trabalho social entende-se, segundo a *International Federation of Social Workers* (2005 *cit. in* APAV, 2013), a promoção da mudança social, da resolução de problemas no contexto das relações interpessoais e da capacidade das pessoas na melhoria do seu bem-estar. O trabalho social procura, assim, introduzir **mudanças positivas no funcionamento psicológico e social de pessoas, grupos e comunidades**, diminuindo vulnerabilidades e proporcionando oportunidades para uma vida social mais satisfatória.

Vários são os propósitos que podem ser apontados ao trabalho social, nomeadamente:

- Facilitar a inclusão de grupos sociais vulneráveis ou em risco;
- Promover o bem-estar e solucionar problemas, intervindo junto de pessoas, grupos e comunidades;
- Desencadear procedimentos de proteção de pessoas que, devido à sua condição ou situação, não se encontrem capazes de o fazer autonomamente.

O trabalho social estende-se, por isso, a áreas muito diversificadas, tais como a educação, a animação, a informação e orientação, o apoio psicossocial e a gestão de serviços ou equipamentos (APAV, 2013).

O Apoio Social é da competência de trabalhadores sociais, em especial dos/as técnicos/as de Serviço Social, mas também de técnicos/as de Política Social e outros profissionais devidamente qualificados da área do Trabalho Social (*idem*).

Como nas demais modalidades especializadas de apoio, o apoio social a vítimas de cibercrime implica que o/a profissional, além da sua formação académica, conheça e domine o enquadramento teórico-concetual das necessidades das vítimas de cibercrime. Além disso, deverá possuir conhecimento e domínio adequados das especificidades e dinâmicas associadas aos diferentes tipos de cibercrime e ao seu impacto junto das vítimas[117].

3.5.3.1. Do diagnóstico social à intervenção individualizada

O **diagnóstico social** constitui um processo de elaboração/sistematização de informação sobre um contexto, compreendendo os seus problemas e necessidades, bem como as causas e a sua evolução. Através do diagnóstico social, será possível estabelecer prioridades e estratégias de intervenção, **envolvendo os meios disponíveis e os atores sociais** (Ander-Egg & Idánez, 1999 *cit in* APAV, 2018).

O diagnóstico social deve constituir uma das primeiras fases do apoio social. Representa um processo contínuo, visando o conhecimento da realidade vivenciada por uma determinada pessoa, grupo ou comunidade, bem como das suas constantes evoluções/modificações, implicando, por isso, a recolha e análise constante de informação.

O **diagnóstico social é uma etapa-base para uma intervenção individualizada** junto da vítima de crime e de cibercrime. Só após a elaboração do diagnóstico sobre a situação relacional, social e institucional da vítima, deverá o/a profissional desenhar a intervenção, envolvendo a vítima e a sua rede de apoio primária, bem como as estruturas formais de apoio (García & Romero, 2012 *cit in* APAV, 2018). Esta abordagem de intervenção individualizada denomina-se Método de Casos.

O Método de Casos pode resumir-se em quatro etapas básicas (*idem*):

- Estudo e diagnóstico do problema;
- Programa/Desenho da intervenção;
- Execução/implementação da intervenção;
- Avaliação.

Para a concretização destas quatro etapas que se materializam na intervenção individualizada nas necessidades relacionais, sociais e institucionais da vítima, o/a profissional deverá:

[117] Veja-se os capítulos 1, 3 e 4 da parte I deste Manual, nos quais são explorados, respetivamente, as tipologias e os diferentes tipos de cibercrime, os fatores de risco associados à experiência de cibervitimação, as consequências da cibervitimação e as necessidades das vítimas de cibercrime.

Quadro II-8: Intervenção individualizada e necessidades das vítimas de crime

Identificar o crime

A identificação da vítima e do crime pode ser efetuada com base na recolha de informação realizada em outros contactos com a entidade[118], na qual se inclui a experiência/história de cibervitimação, mas também informação sobre a vítima, sua caracterização e a história de pré-vitimação.

Avaliar as necessidades da vítima

A avaliação das necessidades individuais e sociais da vítima deve ser efetuada a partir de uma perspetiva centrada nos interesses da vítima, de acordo com o seu contexto de vida e considerando as problemáticas específicas associadas ao seu caso.

O/A profissional deve:

Permitir que a vítima expresse o que deseja e aquilo de que necessita;
Clarificar e reformular as necessidades expressas, de forma a garantir uma correta compreensão;
Transmitir continuamente informação sobre os direitos, recursos e serviços de apoio existentes, que permita à vítima identificar as suas próprias necessidades;
Avaliar continuamente as diferentes necessidades e os seus níveis de urgência, por forma a responder às mais prementes.

As necessidades urgentes incluem: segurança, necessidades básicas, cuidados médicos e/ou psicológicos, acolhimento e apoio jurídico.

As necessidades a médio e/ou longo prazo podem incluir: apoio financeiro, apoio para a educação, apoio na (re)integração, treino de competências e inserção profissional.

Por regra, as necessidades de apoio social ocorrem nas seguintes dimensões:

ACOLHIMENTO	Nas situações de cibercrime possibilitado através da Internet e das TIC com motivações relacionais, como é o caso do *ciber-stalking* e da divulgação não consensual de imagens e vídeos no âmbito de situações de violência nos relacionamentos íntimos, pode haver lugar à necessidade de acolhimento. Este pode ser urgente/de emergência ou programado. O/a profissional deve elaborar o diagnóstico da situação (identificar a rede de primária de apoio - amigos/as, familiares e outras pessoas de confiança - ou a necessidade de se ativarem redes secundárias de apoio) e avaliar o grau de risco daquela situação. O acolhimento pode ter lugar na rede primária de suporte, sempre que esta reúna as necessárias condições de segurança. Pode também ser institucional, o que implica o conhecimento das respostas de acolhimento a nível local/regional/nacional de um determinado país e a articulação/encaminhamento para linhas de emergência social, estruturas/respostas de acolhimento, organizações não-governamentais, serviços da segurança social, entre outras respostas/recursos disponíveis.
ALIMENTAÇÃO	A vítima de cibercrime, por exemplo, nas situações de burla *online*, pode ver-se na impossibilidade económica de fazer face a necessidades básicas, como é o caso de bens alimentares ou de medicação para problemas de saúde pré-existentes. O/A profissional deve efetuar o levantamento das diversas instituições existentes na sua área de intervenção, objetivos, procedimentos e normas de funcionamento, de forma a efetuar um encaminhamento adequado da vítima, acompanhando-a neste contacto com outras instituições/entidades. Para o efeito, o/a profissional deverá conhecer, no seu país, as entidades a quem possa recorrer com vista à resposta às necessidades, o que poderá implicar o contacto/encaminhamento para organizações-não governamentais, serviços da segurança social, instituições religiosas, entre outras respostas/recursos disponíveis.

[118] Veja-se, para o efeito, ponto 2.3. do capítulo 2 da parte II deste Manual.

SAÚDE	A experiência de cibervitimação pode levar ao surgimento de necessidades ao nível da saúde (física e mental). O/A profissional deve ser capaz de identificar, no seu país, as entidades e respostas mais adequadas, o que pode implicar o contacto/encaminhamento para linhas de saúde/emergência, serviços de saúde assegurados pelo Estado, por organizações não-governamentais, por entidades religiosas ou outras respostas ao nível da saúde (inclusivamente serviços privados de saúde).
SITUAÇÃO PROFISSIONAL	Face a potenciais efeitos do cibercrime na situação profissional da vítima, poderá ser necessário encontrar uma nova forma de garantir a sua subsistência. A (re)integração profissional torna-se primordial, de forma a permitir um maior nível de autonomia. O/A profissional deverá avaliar as habilitações académicas da vítima, a sua experiência profissional, as suas preferências relativamente aos setores do mercado de trabalho e eventuais necessidades formativas. Deve proceder ao encaminhamento da vítima junto de entidades competentes, como centros de emprego e formação profissional, que possam auxiliar e promover a reintegração profissional. Deverá também facilitar a articulação da vítima com departamentos de recursos humanos de potenciais contextos de trabalho que se enquadrem no perfil, competências e interesses laborais da vítima.
SITUAÇÃO ESCOLAR/FORMATIVA	O cibercrime pode também colocar em causa a formação/situação escolar da criança/jovem vítima, como é o caso das situações de *ciber-bullying* ou de abuso e exploração sexual de crianças *online*, ou de crianças/jovens a cargo da vítima direta de cibercrime (se tal se aplicar ao caso em concreto). É importante a articulação com os atuais contextos de formação ou escolares, com vista à implementação de ações que permitam a resolução das necessidades de formação das vítimas diretas e indiretas, como a transferência de escola/contexto de formação, de forma sigilosa, de modo a garantir a segurança das vítimas diretas e indiretas.

Encaminhar e trabalhar em cooperação

Estas necessidades básicas (e a resposta às mesmas) constituem áreas de intervenção importantes ao nível do apoio social.

Face às necessidades identificadas e ao âmbito de atuação da entidade na qual o/a profissional exerce as suas funções, poderá ser necessário, como é evidente nas dimensões de apoio anteriormente apresentadas, o encaminhamento/cooperação com outras entidades/respostas existentes na comunidade. O/a profissional (e a entidade na qual exerce as suas funções) deverá possuir, para cada área de intervenção, os contactos de redes de apoio secundárias existentes, a nível regional e nacional, que poderão ser ativadas em benefício do apoio e resposta às necessidades das vítimas de crime.

Com vista a responder às necessidades da vítima e a maximizar a qualidade do apoio prestado, poderá, por isso, ser necessário articular com outros setores/áreas[119], designadamente:

- Segurança Social e Proteção Social (como serviços de segurança social e instituições particulares de solidariedade social/organizações não governamentais);
- Trabalho e Desemprego (incluindo centros de emprego e de formação profissional);
- Departamentos de recursos humanos de empresas e outras organizações ou comissões locais;
- Saúde (como hospitais, centros/unidades de saúde e instituições de saúde mental);
- Educação e Estabelecimentos de Ensino e/ou de Formação;
- Autarquias Locais (câmaras municipais e juntas de freguesia);
- Justiça (tais como, forças policiais, tribunais e gabinetes de medicina legal e forense);
- Comunicação e TIC (incluindo operadoras de telecomunicações, ISP – *Internet Service Providers*, empresas detentoras de redes sociais e outras plataformas de partilha de informação);
- Economia e finanças (como entidades bancárias, entidades emissoras de crédito e empresas e plataformas de pagamentos e transferências eletrónicas).

Essa articulação poderá tomar a forma de encaminhamento ou referenciação[120].

[119] No que diz respeito à coooperacão multissectorial, queira consultar a já mencionada *WePROTECT Global Alliance*, em https://www.weprotect.org/, como exemplo, uma vez que propõem um modelo compreensivo no combate ao abuso e exploração sexual de crianças através da Internet.

[120] Para mais informações sobre a referenciação e o encaminhamento, queira consultar o ponto 3.5.1.3. do capítulo 3 da parte II deste Manual, no qual é abordada a importância da cooperação interinstitucional.

3.5.3.2. Aspetos-chave para o sucesso do trabalho em cooperação

Ainda que a cooperação interinstitucional seja importante no apoio a vítima de cibercrime, independentemente da natureza do apoio em apreço, torna-se especialmente relevante na resposta às necessidades sociais e institucionais identificadas na sequência de uma experiência de vitimação (ou de cibervitimação, neste caso).

DESTAQUE | INFORMAÇÃO EMF FOCO:

No *Policy Paper: challenges in the field of cybercrime and recommendations to overcome them*, desenvolvido ao abrigo do Projeto ROAR: empoderamento das vítimas de cibercrime[121], são propostas recomendações para o desenvolvimento e preparação de estratégias holísticas de cibersegurança. A cooperação multissectorial para uma abordagem centrada na vítima, envolvendo decisores políticos, autoridades policiais, sistemas judiciais, organizações de apoio à vítima, indústria e *media*, é enfatizada enquanto estratégia para uma melhor resposta às necessidades das vítimas de cibercrime e aos desafios associados à cibercriminalidade.

O trabalho em colaboração e cooperação com outros/as profissionais de outras instituições e serviços é fundamental para a qualidade do tratamento prestado a qualquer vítima de crime.

O/A profissional deve trabalhar em colaboração constante com outros profissionais, de outras instituições e serviços, para o correto apoio e adequada resposta aos interesses e necessidades da vítima. Nesse sentido, o/a profissional deve:

- **Facilitar**, promovendo uma comunicação eficaz e uma relação satisfatória entre os/as vários profissionais de diferentes serviços e instituições;

- **Dinamizar**, mobilizando os/as vários profissionais para a resolução/minimização das consequências do crime ou cibercrime e para a adequada resposta às necessidades da vítima.

A atuação integrada evita alguns dos constrangimentos que, por vezes, afetam a cooperação interinstitucional:

A formalidade. Deve diminuir-se os efeitos negativos de uma excessiva formalidade no contacto diário entre as instituições (por exemplo, excesso de trâmites burocráticos), pois esta pode ser prejudicial ao processo de apoio, ao nível da rapidez e da eficácia na resolução do problema.

O tempo. Deve rentabilizar-se o tempo disponível para cumprir determinada exigência do processo (por exemplo: o envio célere de um relatório de encaminhamento;), sem atrasar ou prejudicar o trabalho de outros serviços e instituições.

A falta de sentido prático. Deve promover-se uma visão prática das exigências do processo de

[121] Informação adicional sobre o Projeto, suas principais atividades e resultados estão disponíveis em https://apav.pt/publiproj/index.php/96-projeto-roar .

apoio, ao nível do contacto com outras instituições.

A falta de cordialidade. Deve ser-se gentil com todos os/as profissionais com quem se contacta no âmbito do processo de apoio (por exemplo, ao telefone, pessoalmente, por email, etc.).

Os erros na comunicação. Deve evitar-se comunicações ambíguas que provoquem um entendimento errado das mensagens ou solicitações, pois estas podem criar constrangimentos na relação e prejuízos consideráveis, influenciando a qualidade do apoio prestado à vítima.

A partilha de informação insuficiente. Deve evitar-se a escassez/insuficiências nas informações partilhadas com profissionais de outras instituições ou serviços, pois esta pode limitar ou atrasar o seu trabalho no processo de apoio (por exemplo, enviar um relatório descuidado, omisso ou pouco claro, que não disponha de informações necessárias para trabalhar no processo).

A intervenção redutora e isolada. Deve adotar-se uma visão global no apoio e encaminhamento de vítimas, promovendo o trabalho em rede, através da participação ativa de outros/as profissionais exteriores ao serviço ou instituição, otimizando os recursos disponíveis.

A competição negativa. Não deve ser promovida uma cultura de competição com outros serviços e instituições, mas sim de rentabilização e maximização dos recursos e competências dos mesmos, na promoção de uma intervenção adequada e de qualidade.

A falta de contacto personalizado. Deve, por fim, contactar-se pessoalmente com os/as profissionais de outras instituições e serviços, promovendo-se a aproximação entre todos/as, com vista a facilitar as diligências necessárias na intervenção com vítimas.

4. A IMPORTÂNCIA DA PREVENÇÃO NO COMBATE AO CIBERCRIME

Genericamente, por **prevenção do crime** poderá entender-se todas as iniciativas e esforços, privados e/ou públicos, que visam prevenir o crime, reduzindo o risco da sua ocorrência, através da modificação de fatores de risco, e/ou, quando tal não for possível, minorando os seus efeitos nas pessoas e na sociedade (Copibianco, 2010, Welsh & Farrington, 2012 *cit in* Maia et al., 2016).

As primeiras incursões pela prevenção do crime resultam de abordagens da Saúde Pública, tendo o conceito de *prevenção* (da doença e da enfermidade) sido posteriormente apropriado por outras dimensões da vida social e comunitária (Bloom, 1996, Doll, Saul, & Elder, 2007 *cit in* Saavedra & Machado, 2010) e inclusivamente transposto para matérias relativas à segurança, violência e criminalidade.

4.1. Abordagens para a prevenção do cibercrime: aspetos-chave

No seguimento da referida apropriação do conceito de prevenção, também de acordo com a abordagem de saúde pública (APAV, 2011), esta poderia ser categorizada ***temporalmente*** (ou pela evolução da condição), nas seguintes dimensões:

- **Prevenção primária:** intervenção anterior ao problema, de forma e evitar o seu aparecimento.
- **Prevenção secundária:** intervenção destinada ao tratamento, o mais precoce quanto possível, do problema, considerado que o mesmo se encontra já presente.

  Na sua transposição para as questões da violência e do crime, a prevenção secundária diz respeito a abordagens centradas nas reações imediatas ao crime e à violência (ex.: cuidados médicos; serviços de emergência).

- **Prevenção terciária:** intervenção centrada no evitamento da recaída, prevenindo a frequência e severidade dos danos.

  A prevenção terciária, na sua aplicação às questões da violência e da criminalidade, contempla abordagens focadas nos cuidados prolongados após a violência ou crime, como a reabilitação, a reintegração e a diminuição do trauma/consequências associadas ao crime/violência.

Apesar de, tradicionalmente, as abordagens de prevenção secundária e terciária do crime e da violência serem utilizadas para a intervenção junto das vítimas, também são consideradas relevantes para a intervenção junto dos/as autores/as do crime ou da violência, nomeadamente no âmbito das respostas do setor judicial.

A prevenção pode também ser definida de acordo com o ***grupo alvo de interesse*** ou ***população*** a quem se destina (APAV, 2011), sendo categorizada como:

- **Prevenção universal:** abordagens que visam grupos ou a população em geral, independentemente do nível de risco.

  Pode referir-se, como exemplo de abordagens de prevenção universal, os programas de prevenção da violência destinados a crianças/jovens de um determinado nível de ensino, bem como campanhas de sensibilização dirigidas à população.

- **Prevenção seletiva:** abordagens destinadas a grupos/pessoas consideradas em maior risco de envolvimento em situações de violência ou crime, comparativamente com a população em geral.

  Entre os exemplos desta abordagem de intervenção, encontram-se os programas de promoção de competências parentais para famílias monoparentais.

- **Prevenção indicada:** abordagens de intervenção junto de pessoas/grupos de alto risco, que já demonstraram algum envolvimento em situações de violência ou crime, seja enquanto vítimas e/ou como autores/as.

  A título exemplificativo, nas abordagens de prevenção indicada, podem incluir-se os programas de intervenção para pessoas acusadas do crime de violência doméstica e as respostas de apoio para vítimas de crime e violência proporcionadas por estruturas e organizações de apoio à vítima.

Existem igualmente outras tipologias de classificação das estratégias de prevenção, nomeadamente em função do ***foco da prevenção*** (e.g., ONU, 2011 *cit in* Maia et al., 2016; Tonry & Farrington, 1995 *cit in* Maia et al., 2016), tais como:

- **Prevenção criminal através do desenvolvimento social**, centrada no aumento dos fatores de proteção e na redução dos fatores de risco da criminalidade, na qual se pode incluir, por exemplo, os programas de promoção de competências sociais para crianças em risco.

- **Prevenção criminal comunitária ou local**, centrada na intervenção em zonas geográficas com maior risco de criminalidade e na promoção do sentimento de segurança.

- **Prevenção criminal situacional**, que diz respeito à redução de oportunidades para a prática de crimes, ao aumento dos riscos/custos associados ao seu cometimento e à redução dos benefícios.

- **Prevenção criminal pela justiça criminal**, na qual se poderão incluir os programas de reintegração e de prevenção da reincidência no crime.

Com exceção feita às estratégias de prevenção criminal comunitária ou local, qualquer outra das demais abordagens acima indicadas de prevenção do crime pode ser transposta para a **prevenção da cibercriminalidade**. Ainda assim, importa salientar que os esforços para a prevenção do cibercri-

me concentram-se frequentemente na tecnologia e na proteção de computadores e dispositivos, ao passo que os modelos de prevenção do crime se centram principalmente no fator humano.

Independentemente das abordagens à prevenção e das tipologias anteriormente sintetizadas, a abordagem de Saúde Pública[122] é útil para auxiliar as entidades e organizações a compreender e a implementar estratégias de prevenção do crime e da violência. Pese embora a complexidade da prevenção, poderemos organizar em quatro macro-etapas o planeamento, preparação e implementação de estratégias de prevenção:

1	
definir o problema	• implica **compreender o fenómeno** e as suas dinâmicas, mas também identificar a sua **dimensão e expressão** (ex: dados estatísticos sobre o número de denúncias de um determinado crime junto das autoridades) num determinado grupo, comunidade, região ou país
2	
identificar os fatores de risco e os fatores de proteção	• **fatores de risco:** características ou condições que podem aumentar a probabilidade de aparecimento ou ocorrência de um determinado problema • **fatores de proteção:** características ou condições que podem diminuir a probabilidade de aparecimento ou ocorrência de um determinado problema • as estratégias de prevenção deverão reduzir os fatores de risco e aumentar os fatores de proteção
3	
desenvolver, testar e avaliar estratégias de prevenção	• as estratégias de prevenção devem ser desenvolvidas com base em evidências teóricas e considerando os diagnósticos efetuados, bem como o problema que se pretende resolver e os faotres de rico e proteção associados • **monitorizar e avaliar a eficáci**a das estratégias de prevenção são passsos fundamentais
4	
disseminar e generalizar	• depois de analisados os resultados das estratégias de prevenção implementadas, é fundamental a sua **divulgação**, para que outras entidades e organizações as possam utilizar

Figura II-6: Etapas para o planeamento e implementação de estratégias de prevenção

Adicionalmente, no que diz respeito à prevenção do cibercrime, o modelo proposto por Askerniya (2012) para a **organização das estratégias de prevenção da cibercriminalidade** apresenta quatro dimensões-chave, que integram, transversalmente, a consciencialização e a educação enquanto elementos críticos na redução do cibercrime (Jahankhani, 2013 cit in Al-Ali et al., 2018):

1. O nível de **conhecimento técnico dos/as utilizadores/as individuais** é a primeira dimensão das intervenções de prevenção do cibercrime. Com o objetivo de reduzir o risco individual e melhorar a proteção pessoal, as intervenções devem concentrar-se na educação, na consciencialização e no treino dos/as utilizadores/as relativamente a competências específicas necessárias para a participação segura em diferentes atividades *online* (tais como, o *download* de músicas, jogos e filmes, as compras *online* e/ou a utilização das redes sociais).

[122] Informação detalhada sobre a Abordagem de Saúde Pública na prevenção do crime e da violência, bem como recursos de apoio ao planeamento, implementação e avaliação de medidas de prevenção estão disponíveis em https://vetoviolence.cdc.gov/apps/main/home.

2. A segunda dimensão diz respeito à redução da exposição ao risco de cibercrime através de **estratégias de prevenção adaptadas aos diferentes estádios individuais de desenvolvimento** do/a utilizador/a. Na base desta dimensão, encontra-se a premissa de que o risco de cibervitimação é impactado pelos fatores de risco e de proteção associados ao desenvolvimento individual, assumindo-se, como tal, a idade/faixa etária do/a utilizador/a enquanto elemento-chave para a definição e decisão em relação às estratégias de intervenção preventiva do cibercrime a colocar em prática.

3. A terceira dimensão diz respeito aos **níveis de risco dos/as utilizadores/as face à exposição ao cibercrime** e ao grau em que as intervenções preventivas são necessárias, com foco nos seus níveis de conhecimento, treino e consciencialização. Nesse sentido:

    - O **baixo risco de exposição ao cibercrime** está associado a utilizadores/as que possuem um conhecimento considerável relativamente às TIC e à Internet, bem como níveis ajustados de consciencialização relativamente aos riscos da exposição *online*.

    - O **risco médio de exposição ao cibercrime** associa-se a utilizadores/as com conhecimento e consciencialização insuficientes relativamente aos riscos da exposição *online* e com risco mais elevado (nomeadamente, em comparação com a categoria anterior) de cibervitimação. Nesta dimensão de risco de exposição ao cibercrime, enquadram-se as pessoas que, pese embora os seus conhecimentos sobre a segurança de computadores e dispositivos, não possuem a consciencialização necessária para alterar o seu comportamento *online* e/ou hábitos de utilização da Internet e das TIC.

    - O **risco elevado de exposição ao cibercrime** associa-se a utilizadores/as com índices elevados de utilização intensiva da Internet e das TIC, mas com reduzida consciencialização face à exposição ao risco.

4. A quarta e última dimensão deste modelo diz respeito à **promoção de competências e comportamentos individuais e ao desenvolvimento de intervenções** assentes no treino, na educação e na consciencialização para os riscos relativos à exposição *online* e à adoção de determinados comportamentos[123].

Apresentaremos, nos campos seguintes, algumas práticas de prevenção do cibercrime.

4.2. A informação, a sensibilização e a educação enquanto estratégias de prevenção

No seguimento das dimensões-chave das estratégias de prevenção do cibercrime, anteriormente apresentadas, torna-se clara a importância da informação, da sensibilização e da educação de utili-

[123] Para informação adicional relativamente à vulnerabilidade enquanto fator de risco para a cibervitimação, queira consultar ponto 3.2 do capítulo 3 da parte I deste Manual.

zadores/as da Internet e das TIC para o seu papel (ou melhor, para o papel dos seus comportamentos e das suas competências) no aumento/redução do risco de exposição ao cibercrime.

A perceção dos/as utilizadores/as da Internet e das TIC relativamente às suas próprias **capacidades e conhecimentos** para se protegerem da cibervitimação afeta o seu comportamento e as suas atividades *online*. O mesmo se aplica à responsabilização pela segurança pessoal *online* (Boehmer et al., 2015; LaRose & Rifon, 2007). Dito de outra forma, as pessoas que consideram que a cibersegurança constitui uma responsabilidade que também é pessoal e/ou que entendem dispor dos conhecimentos e capacidades necessárias para se protegerem da cibervitimação, adotam (provavelmente) mais medidas de cibersegurança e mais comportamentos de proteção pessoal aquando da utilização da Internet e das TIC.

Esta leitura destaca a necessidade de realização de **campanhas de informação e de sensibilização** e da implementação de **programas educativos** (Martin & Rice, 2011; Burns & Roberts, 2013):

- As campanhas de informação e sensibilização deverão promover o uso seguro e competente da Internet e das TIC;
- Os programas educativos devem fornecer conhecimento e oportunidades para o treino e assimilação de competências necessárias para a adoção de comportamentos de segurança *online*.

Em qualquer dos casos, estas estratégias de informação, sensibilização e educação deverão (Bandura, 1997 *cit in* Lee et al., 2008; Boehmer et al., 2015; Saridakis et al., 2016):

- Informar, de forma explícita, relativamente aos riscos a que os/as utilizadores/as podem estar sujeitos face à utilização da Internet e das TIC;
- Identificar e consciencializar os/as utilizadores/as para os comportamentos pessoais de risco que podem aumentar a vulnerabilidade à cibervitimação;
- Sensibilizar os/as utilizadores/as para as medidas de proteção e de cibersegurança existentes, incluindo através de informação objetiva sobre a eficácia da proteção disponível;
- Instruir sobre as formas de implementação das medidas de proteção e cibersegurança disponíveis, nomeadamente através de ajuda contextual e de instruções passo-a-passo, por exemplo;
- Enfatizar os resultados positivos associados à adoção de comportamentos seguros *online*.

Sendo verdade que as estratégias de informação, sensibilização e educação são passíveis de ser implementadas em qualquer faixa etária, as práticas e iniciativas neste domínio têm-se sobretudo dedicado à informação, sensibilização e educação de crianças e jovens.

Apresentamos em seguida, por isso mesmo, uma síntese de algumas práticas de prevenção universal do cibercrime, incluindo iniciativas, programas e projetos, para crianças de diferentes faixas etárias, assentes na informação, na promoção de conhecimento e no reforço de competências para uma utilização segura da Internet e das TIC.

Quadro II-9: Programas e projetos de prevenção do cibercrime - COMUNICAR EM SEGURANÇA

Tipo de prevenção	Universal
População-alvo	Crianças com idades compreendidas entre os 6 e os 18 anos com extensão a pais e a população sénior.
Temas/Problemas	Segurança na Internet
Objetivos	• Promover competências em TIC • Iniciativa de voluntariado empresarial da Fundação Altice que pretende alertar a comunidade educativa para a utilização correta e segura das tecnologias de informação, designadamente Internet e telemóvel.
Contexto de implementação	O programa integra sessões de sensibilização em sala de aula com conteúdos estruturados por ano e abrangendo todos os ciclos e uma peça de teatro. É complementado por diversos recursos *online*.
Descrição	Parceria: PSP - Polícia de Segurança Pública Consórcio CIS - Centro Internet Segura, Portugal ANPRI – Associação Nacional de professores de Informática RBE – Rede de Bibliotecas Escolares Temas abordados: • Controle parental • Privacidade • *Password* • ID digital • Partilha de dados pessoais e de fotos • *Ciber-bullying* • Utilização saudável • Segurança dos dispositivos (Telemóvel e PC) • Instalação de *apps* e jogos • Fraude/ Virus • Compras *Online* • *Malware* • *Ransomware* • *Wi-Fi* público
País de implementação	Portugal
Informação adicional	https://fundacao.telecom.pt/Site/Pagina.aspx?PageId=1975

Quadro II-10: Programas e projetos de prevenção do cibercrime - THINKUKNOW – "JESSIE & FRIENDS"

Tipo de prevenção	Universal
População-alvo	Crianças com idades compreendidas entre os 4 e os 7 anos
Temas/Problemas	Segurança na Internet
Objetivos	• Promover conhecimento, competências e confiança para uma utilização segura e protegida da Internet e das TIC; • Proporcionar oportunidades para aprendizagem de princípios/valores-chave para uma utilização segura da Internet e das TIC: respeito pelos outros; consentimento; comportamento saudável e não saudável na Internet; procura de ajuda junto de pessoa adulta de confiança.
Contexto de implementação	Pode ser implementada em grupo (em contexto de sala de aula, por exemplo) e individualmente (contexto familiar)
Descrição	• "Jessie & Friends" é uma série de animação, com três episódios para crianças dos 4 aos 7 anos de idade: (i) episódio 1 – 4-5 anos; (ii) episódio 2 – 5-6 anos e (iii) episódio 3 – 6-7 anos. • "Jessie & Friends" acompanha as aventuras de Jessie, Tia e Mo, quando estas utilizam a Internet e as TIC. As personagens aprendem que, embora a Internet seja um contexto de divertimento, também é um contexto de risco. • A série é acompanhada por um Guia para professores, pais e/ou responsáveis, com orientações para as sessões. • É também complementado por um livro com as histórias, que permite o reforço das aprendizagens em casa/em família e/ou na escola
País de implementação	Reino Unido
Informação adicional	https://www.thinkuknow.co.uk/professionals/resources/jessie-and-friends/

Quadro II-11: Programas e projetos de prevenção do cibercrime - THINKUKNOW – "THINKUKNOW TOOLKIT"

Tipo de prevenção	Universal
População-alvo	Jovens de 11 anos ou mais anos
Temas/Problemas	Segurança na Internet
Objetivos	• Desenvolver abordagens saudáveis relativamente a temas, como: relacionamentos, sexo e Internet; • Identificar comportamentos negativos associados a esses temas; • Saber onde encontrar conselhos e orientações sobre estes temas; • Saber onde procurar ajuda, perante situações de risco online.
Contexto de implementação	Contexto escolar
Descrição	São realizadas atividades: • *Speed finding* - interpretação de papéis, que explora a natureza da "amizade" *online*, identifica riscos e destaca formas seguras de socializar *online*; • *Digital Tatto* - discussão em pares e grupo, apresentando aos jovens o conceito de "tatuagem digital" (ou "pegada digital") e formas de a gerir; • *Code Breaker* - atividade onde os/as jovens tentam adivinhar as senhas definidas por personagens fictícias; • *Thinkuknow Better?* - jovens desenvolvem conselhos para apoiar os pares.
País de implementação	Reino Unido
Informação adicional	https://www.thinkuknow.co.uk/professionals/resources/thinkuknow-toolkit/ https://www.src.ac.uk/images/news/658x300/1920/Aug19/StudAct/Thinkuknow_Toolkit.pdf

Quadro II-12: Programas e projetos de prevenção do cibercrime - THINKUKNOW – "JOSH & SUE"

Tipo de prevenção	Universal
População-alvo	Jovens com idades compreendidas entre os 11 e os 13 anos com dificuldades de aprendizagem
Temas/Problemas	Segurança na Internet
Objetivos	• Os/As jovens devem ser capazes de perceber as consequências associadas a atitudes/condutas inadequadas *online*, explorando-se comportamentos de segurança *online* e comportamentos positivos nas relações interpessoais *online*
Contexto de implementação	Contexto escolar e/ou familiar
Descrição	• O filme está disponível em duas versões, para jovens com diferentes níveis de dificuldades de aprendizagem. • O filme pode ser utilizado em contexto escolar e/ou em família.
País de implementação	Reino Unido
Informação adicional	https://www.thinkuknow.co.uk/parents/Support-tools/Films-to-watch-with-your-children/Josh_and_Sue_original1/

Quadro II-13: Programas e projetos de prevenção do cibercrime - ZUKY'S SAFETY GUIDE

Tipo de prevenção	Universal
População-alvo	Crianças (sem especificação de idade)
Temas/Problemas	Segurança na Internet
Objetivos	• Informar as crianças sobre os riscos existentes na Internet e sobre as estratégias de cibersegurança e comportamentos de proteção pessoal
Contexto de implementação	Pode ser implementado em qualquer contexto, pela família, responsáveis e/ou profissionais
Descrição	• Série de animação para crianças, onde a personagem principal é o "Zuky", um super herói da segurança na Internet. Esta série pode ser visualizada no *website* oficial ou no Youtube®. Ao utilizar o *website* oficial, para além dos vídeos, também são disponibilizados guias e *quizzes* para as crianças, assim como conselhos para famílias e responsáveis legais sobre segurança na Internet.
País de implementação	Holanda
Informação adicional	Informação adicional https://www.paloaltonetworks.com/campaigns/kids-in-cybersecurity https://www.youtube.com/channel/UCDYFyxEbTw0oFOFdzP1hlfg https://trailhead.gsnorcal.org/wp-content/uploads/2018/12/EN_PANE_0nepaper_Kids_in_Cybersecurity.pdf

Quadro II-14: Programas e projetos de prevenção do cibercrime - PROJETO DESHAME

Tipo de prevenção	Universal
População-alvo	Jovens com idades compreendidas entre os 13 e os 17 anos
Temas/Problemas	Assédio sexual *online*
Objetivos	• Promover a denúncia de situações de assédio sexual *online*[124] entre jovens • Melhorar a cooperação multissetorial na prevenção e a resposta a esse comportamento
Contexto de implementação	Contexto comunitário e escolar
Descrição	O Projeto deSHAME é financiado pela Comissão Europeia e visa combater o assédio sexual *online*. É uma colaboração entre a *Childnet* (Reino Unido), *Save the Children* (Dinamarca), *Kek Vonal* (Hungria) *e UCLan* (Reino Unido). Envolve o desenvolvimento de recursos educativos variados, com vista a prevenir o assédio sexual online e a capacitar para a denúncia. No seu âmbito, foi desenvolvido o *toolkit Step Up, Speak Up!* - uma ferramenta com sessões práticas para abordar a problemática do assédio sexual *online* junto de jovens. Foram também desenvolvidos diversos recursos e materiais de apoio para o contexto escolar.
País de implementação	Vários
Informação adicional	https://www.childnet.com/our-projects/project-deshame https://www.childnet.com/ufiles/Project_deSHAME_Dec_2017_Report.pdf

[124] O projeto define assédio sexual *online* como um conjunto de condutas sexuais não desejadas que têm lugar em qualquer plataforma digital. Este conceito abrangente incorpora diferentes formas de cibercrime/violência abordadas no capítulo 1 da parte I deste Manual, incluindo *ciber-bullying*, divulgação não consensual de imagens e vídeos e diferentes formas de abuso e exploração sexual de crianças através da Internet.

Quadro II-15: Programas e projetos de prevenção do cibercrime - KIDS IN THE KNOW - "ZOE & MOLLY *ONLINE*"

Tipo de prevenção	Universal
População-alvo	Alunos/as do 1º ciclo de ensino
Temas/Problemas	Segurança na Internet
Objetivos	• Os/As alunos/as devem ser capazes de identificar os riscos e os benefícios na utilização da internet • Os alunos devem ser capazes de responder com segurança aos riscos que encontram online
Contexto de implementação	Contexto escolar Também possui um *website* com jogos, *quizzes* e banda desenhada, que pode ser utilizado em contexto escolar, como complemento, ou em contexto familiar.
Descrição	• *"Zoe & Molly Online"* é uma banda desenhada. Desenvolvida pelo *Canadian Centre for Child Protection*, *"Zoe & Molly Online"* foi projetado para promover discussões em sala de aula sobre os riscos associados à partilha de informações pessoais *online*. • Promove o envolvimento e a supervisão de pessoas adultas, incentivando as crianças a verificar sempre com uma pessoa adulta de confiança antes de compartilhar informações *online* com qualquer pessoa.
País de implementação	Canadá
Informação adicional	http://www.zoeandmolly.ca/pdfs/zm_TeacherKit_SinglePagesGr4_en.pdf https://www.zoeandmolly.ca/app/en/

4.2.1. O exemplo das campanhas públicas de informação e sensibilização

Os meios de comunicação social são instrumentos poderosos de divulgação, assumindo um papel de relevo na prevenção da violência e do crime, em diferentes dimensões (APAV, 2011).

Os *media* podem, por isso, constituir um importante canal na prevenção do cibercrime, nomeadamente através da disseminação de campanhas públicas de informação e sensibilização sobre a temática, seja através de diferentes meios de comunicação, incluindo a Internet e as redes sociais, bem como outros mais tradicionais, como a televisão. De todo o modo, as campanhas de informação e sensibilização devem ser utilizadas como parte de uma abordagem mais ampla de prevenção do cibercrime (Brewer et al., 2019).

As campanhas podem ter objetivos diversos (Finn & Banach, 2000; Brewer et al., 2019), como:

- Transmitir informação sobre medidas de cibersegurança e comportamentos pessoais de proteção para a utilização da Internet e das TIC;

DESTAQUE | PRÁTICAS EM FOCO:

A European Network and Information Security Agency (ENISA) promove anualmente a campanha de sensibilização *European Cyber Security Month*.

Esta campanha europeia procura sensibilizar para as ameaças à cibersegurança e promover a cibersegurança junto de pessoas e organizações.

Ao abrigo desta campanha, há também lugar à disponibilização de recursos sobre proteção pessoal, bem como a diferentes iniciativas de educação e de partilha de boas práticas.

As diversas campanhas realizadas, bem como os recursos associados, incluindo vídeos e infografias, estão disponíveis em https://cybersecuritymonth.eu/press-campaign-toolbox/infographics.

Informação completa sobre a iniciativa *European Cyber Security Month* está disponível em: https://cybersecuritymonth.eu/.

- Promover comportamentos e valores positivos associados à utilização da Internet e das TIC;

DESTAQUE | PRÁTICAS EM FOCO:

Ainda ao abrigo da campanha *European Cyber Security Month* de 2019, o mote da ciber-higiene é utilizado para informar e sensibilizar relativamente à importância de uma utilização saudável e segura das TIC e da Internet no dia-a-dia.

Os materiais desta campanha podem ser acedidos em: https://cybersecuritymonth.eu/#/campaign.

A campanha *European Cyber Security Month* e a *European Network and Information Security Agency* disponibilizam uma série de recursos de informação e sensibilização.

De entre eles, destaca-se o *Network and Information Security (NIS) QUIZ*: uma ferramenta de autodiagnóstico que permite avaliar os níveis de conhecimento e competências sobre matérias como a cibersegurança em geral, a privacidade e as ameaças à cibersegurança.

Esta ferramenta, disponível em várias línguas, pode ser acedida e utilizada em: https://cybersecuritymonth.eu/references/quiz-demonstration/welcome-to-the-network-and-information-security-quiz/.

- Informar sobre os comportamentos a adotar em situações de cibervitimação;

DESTAQUE | PRÁTICAS EM FOCO:

A campanha de sensibilização pública *Say No!* da EUROPOL visa a consciencialização e sensibilização de crianças e jovens para a identificação e atuação perante situações de extorsão sexual de crianças *online*, reforçando a importância da denúncia e da procura de apoio.

Os vídeos da campanha (em diversas línguas) e outros recursos informativos estão disponíveis em: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/online-sexual-coercion--and-extortion-crime.

- Promover o envolvimento coletivo ou de terceiros na proteção e segurança *online* (por exemplo, o papel da família na identificação do risco associado aos comportamentos online dos/as seus filhos/as);
- Dissuadir a prática de cibercrimes, fornecendo informação relativamente aos riscos e consequências negativas associadas.

DESTAQUE | PRÁTICAS EM FOCO:

Também a EUROPOL, com um registo e objetivo distintos, lançou a campanha de sensibilização *Cyber crime vs cyber security: what will you choose?*.

Disponível em diferentes línguas, esta campanha, também dirigida à população jovem, visa a dissuasão face ao envolvimento no cibercrime, salientando as consequências e custos associados ao envolvimento nesse tipo de comportamentos ilícitos.

O material da campanha está disponível para *download* em: https://www.europol.europa.eu/publications-documents/cyber-crime-vs-cyber-security-what-will-you-choose-poster

Ao abrigo da iniciativa, a EUROPOL disponibiliza também informação e aconselhamento para a população jovem, assim como para educadores/as e famílias.

4.3. O papel da família na prevenção

As pessoas adultas não nasceram, ao contrário das crianças e jovens, "nativos digitais", pelo que não têm a mesma aceitação automática da Internet e das TIC enquanto algo natural, fundamental e inquestionável na sua existência. Adicionalmente, para além das limitações em matéria de conhecimento e competências para uma utilização eficaz e eficiente da Internet e das TIC, a família não tem, com frequência, uma consciência clara das atividades *online* praticadas pelas crianças e jovens a seu cargo (Richardson & Milovidov, 2019; Cross et al., 2016; Lwin et al., 2013; Öztürk & Akcan, 2016). Paradoxalmente, desempenham um papel fundamental na informação e educação das crianças e jovens relativamente à utilização segura e consciente da Internet e das TIC e, consequentemente, na prevenção

da cibervitimação e da adoção de comportamentos de risco *online* (Mesch, 2009; Notar et al., 2013; Morais, 2012 *cit in* Martins et al., 2017; Smallbone & Wortley, 2017; Richardson & Milovidov, 2019).

A intervenção da família é, por isso, muito importante:

- Na definição e implementação de **regras consistentes** de utilização da Internet e das TIC por parte das crianças e jovens a cargo;
- Na educação das crianças e jovens sobre os **direitos e responsabilidades** aquando da utilização da Internet e das TIC;
- Na **promoção da empatia** e do respeito pelo outro em qualquer contexto, inclusivamente online;
- Na transmissão de **informação** e capacitação das crianças e jovens para as questões da privacidade, cibersegurança e proteção pessoal aquando da utilização da Internet e das TIC, bem como na **apresentação clara dos riscos associados** à utilização da Internet e das TIC, inclusivamente em matéria de violência e crime;
- Na **supervisão da utilização da Internet e das TIC**, através de uma comunicação aberta, da aprendizagem do uso da Internet e das TIC e do interesse pelas atividades *online* realizadas pelas crianças e jovens a cargo;
- No reconhecimento, junto das crianças e jovens a seu cargo, de eventuais **indicadores de cibervitimação** (ou de uma utilização não saudável das TIC e da Internet), facilitando a adequada intervenção/proteção da criança ou jovem em situações de cibercrime;
- Na manutenção de **canais comunicacionais** com as crianças e jovens, por forma a promover a procura de apoio/ajuda junto de pessoas adultas de confiança perante situações de cibervitimação e outras circunstâncias em que a proteção pessoal na Internet e nas TIC possa estar comprometida.

DESTAQUE | PRÁTICAS EM FOCO:

A *INTERNETMATTERS.ORG* é uma organização sem fins lucrativos que tem como objetivo capacitar famílias para manter as crianças e jovens em segurança aquando da utilização da Internet e das TIC.

A plataforma dispõe de informação, aconselhamento e diversos recursos específicos para famílias com crianças e jovens de diferentes faixas etárias.

Dispõe ainda de informação sobre diferentes fenómenos de cibercrime que podem afetar crianças e jovens, como o *grooming online, o ciber-bullying*, o furto de identidade *online*, entre outros.

A plataforma está disponível em: https://www.internetmatters.org/.

PARENTINFO.ORG é também uma plataforma dirigida a pais e famílias, com informação e aconselhamento em torno de um conjunto de temáticas de interesse relacionadas com a Internet e as TIC, contemplando matérias como a cibersegurança, aplicações e tecnologia, bem-estar e saúde, entre outros.

A plataforma está disponível em: https://parentinfo.org/.

Ainda no que respeita ao papel da família na prevenção do cibercrime, é introduzido o conceito de *parentalidade digital*, que pode ser operacionalizado como:

- Comunicação aberta entre a família/pais e as crianças e jovens a seu cargo;
- Envolvimento da família/pais nas atividades *online* realizadas pelas crianças e jovens, do mesmo modo que esse envolvimento tem lugar nas atividades quotidianas das crianças e jovens nos contextos *tradicionais*;
- Proteção da presença digital das crianças e jovens a seu cargo, isto é, do modo como a criança ou jovem se apresenta ou retrata nas suas atividades *online*;
- Aprendizagem mútua entre a família/pais e as crianças e jovens a seu cargo;
- Proteção das crianças e jovens a cargo relativamente aos riscos e ameaças da Internet e das TIC, nomeadamente em matéria de cibercriminalidade.

DESTAQUE | PRÁTICAS EM FOCO:

O Conselho da Europa lançou o *Parenting in the Digital Age* Parental – *Practical guidance for the online protection of children from sexual exploitation and sexual abuse*.

Trata-se de um guia com boas práticas para pais e famílias, no qual são abordadas diferentes formas de abuso e exploração sexual de crianças através da Internet. De forma prática e informativa, este guia partilha dicas e recursos que visam auxiliar pais e famílias na proteção das crianças e jovens a cargo face a estes fenómenos e inclusivamente na atuação perante situações em que a cibervitimação já tenha ocorrido.

O guia está disponível em https://rm.coe.int/digital-parenting-/16807670e8.

O Conselho da Europa disponibiliza ainda uma série de outros recursos informativos e pedagógicos relativamente à proteção de crianças e jovens na Internet. Sugere-se, nesse âmbito, o *Internet Literacy Handbook*, também do Conselho da Europa, disponível para *download* em: https://www.coe.int/en/web/children/internet-literacy-handbook.

Veja-se https://www.coe.int/en/web/children/the-digital-environment, para informação adicional.

4.4. A escola enquanto contexto privilegiado de prevenção

A escola, a par da família, é um **contexto de socialização muito importante** para o desenvolvimento das crianças e jovens, não somente no que se refere a aprendizagens curriculares, mas também no que diz respeito à aprendizagem de **competências sociais para a vida**, isto é, de competências fundamentais para o funcionamento e comportamento da criança ou jovem em relação ao mundo que a rodeia (Saavedra & Machado, 2010), nomeadamente aos seus contextos relacionais mais próximos, como o grupo de pares e a família, mas também, de forma mais abrangente, no seu funcionamento em sociedade. Diga-se também a qualidade do vínculo entre a criança ou jovem e a escola é fator de

proteção face ao envolvimento em comportamentos de risco, motivo pelo qual se torna particularmente importante a promoção de oportunidades, em contexto escolar, para o reforço do bem-estar e de relacionamentos positivos das crianças e jovens face aos seus pares e aos/às profissionais de educação (McNeely, Nonnemaker, & Blum, 2002 *cit in* Saavedra & Machado 2010).

A escola é assim um contexto natural para a implementação de iniciativas de prevenção do crime e da violência, uma vez que a maioria das crianças frequenta a escola e "vive" nesse contexto uma parte significativa do seu tempo (Durlak, 1995 *cit in* idem).

Apresentamos, em seguida, um conjunto de características que se entendem como desejáveis para a eficácia de programas de prevenção em contexto escolar (APAV, 2011; Brewer et al., 2019):

Quadro II-16: Principais características a considerar nos programas de prevenção em contexto escolar

Base teórica coerente: o ponto de partida para o planeamento deverá ser uma base teórica clara e com evidências de sucesso proporcionadas pela investigação.

Abordagem ecológica: a atenção do programa deverá incidir não apenas no indivíduo, mas também nos contextos sociais nos quais este se movimenta: família, escola, comunidade. Os programas de intervenção na escola têm mais sucesso quando complementados com intervenções na família e na comunidade, uma vez que estes poderão reforçar e promover as mudanças de comportamento.

Abordagem integrada dos fatores de risco e dos fatores de proteção: os programas devem ser desenvolvidos de modo a reduzirem os fatores de risco e a promoverem os fatores de proteção.

Atenção individualizada: a intervenção deve ser planeada de acordo com as necessidades específicas do indivíduo/grupo; os programas devem ser adequados à idade, nível de desenvolvimento e características dos grupos-alvo.

Intervenção precoce e desenvolvimentalmente ajustada: a intervenção deverá ser o mais precoce possível, de acordo com o nível de desenvolvimento dos indivíduos.

Escolha adequada dos alvos de mudança: o aumento de conhecimento, a mudança de atitudes, a mudança de comportamentos e a aprendizagem de novas competências são os alvos de mudança mais comuns.

Envolvimento dos pares: dada a influência dos pares, há programas de prevenção assentes na ação dos grupos de pares como agentes preventivos.

Utilização de métodos interativos de transmissão de informação: devem realizar-se atividades com um formato interativo, apelativo e adequado à faixa etária dos grupos-alvo: grupos de discussão, debates, *brainstorming*, *role-play*, etc..

Aprendizagem e treino sistemático de competências: devem ser proporcionadas oportunidades para o treino de competências sociais: resolução de conflitos, assertividade, tomada de decisão, escuta ativa, bem como o seu treino através da adoção de estratégias cognitivo-comportamentais, tais como *role-play*, simulação de situações próximas da realidade e das experiências pessoais dos sujeitos, etc..

Promoção de consciência social: os programas de prevenção deverão ajudar os/as destinatários/as a compreenderem as emoções e pensamentos dos outros (empatia) e a apreciarem a interação positiva com diferentes grupos.

Gestão das emoções: os programas de prevenção deverão auxiliar os/as participantes a lidar adequada e eficientemente com as emoções (autogestão emocional).

Focalização nos relacionamentos: os programas de prevenção deverão preparar os/as participantes para o estabelecimento de relacionamentos positivos com os outros, promovendo a sua capacidade de comunicarem, cooperarem, negociarem soluções para conflitos, procurarem ajuda (se necessário) e resistirem de forma apropriada à pressão dos pares e aos desafios do meio.

Formação, supervisão e trabalho multidisciplinar: a preparação dos/as profissionais é fundamental para a qualidade e o sucesso da implementação.

Neutralidade na abordagem do género: é importante respeitar a identidade de género dos/as destinatários e considerar esta variável no processo de intervenção.

Focalizar nos níveis normativos das problemáticas: para lá das formas mais graves ou severas da violência, os programas de prevenção devem abordar os níveis "normativos" de violência (nomeadamente as formas de violência subtis e habitualmente toleradas ou normalizadas pelo grupo-alvo da intervenção).

Alternativas de comportamento: a intervenção deverá apresentar alternativas de comportamento incompatíveis com o uso de comportamentos inadequados.

Informação: os programas devem prever também a transmissão de conhecimentos sobre os fatores de risco e as consequências de determinado comportamento e sobre as estruturas sociais de apoio.

Clareza dos conteúdos e simplicidade dos materiais: o programa deverá dispor de guias e/ou manuais estruturados de apoio à implementação, de fácil utilização.

Implementação completa dos conteúdos: os programas devem ser implementados na sua totalidade e cumprindo os objetivos propostos, devendo prever-se mecanismos de monitorização da sua implementação.

Intervenção intensiva e longo prazo: os programas de prevenção devem ser intensivos e a longo prazo.

Avaliação: os programas de prevenção devem prever a medição independente (externa à equipa responsável pela sua criação/implementação), através de metodologias sustentadas, das mudanças atingidas nos grupos-alvo.

Sustentabilidade: também é importante avaliar os custos *versus* benefícios da implementação e a sua sustentabilidade a longo-prazo.

DESTAQUE | PRÁTICAS EM FOCO:

O Programa *NoTrap!* é um programa italiano de intervenção online e em contexto escolar desenvolvido com o objetivo de prevenir e combater o *bullying* e o *ciber-bullying*.

O ponto de partida do programa advém das TIC, tendo duas assunções de base:

- A utilização das TIC pode aumentar o risco de *ciber-bullying*.
- As TIC podem ser também utilizadas como ferramenta de treino e reforço de conhecimentos e competências de prevenção e atuação face ao *ciber-bullying*.

Os estudos de avaliação têm identificado resultados positivos da implementação do programa na redução da vitimação por *bullying* e na cibervitimação por *ciber-bullying* (Palladino et al., 2016).

DESTAQUE | PRÁTICAS EM FOCO:

O Projeto *CyberTraining: A Research-based Training Manual On Ciber-bullying* trabalhou especificamente a problemática do *ciber-bullying*, tendo contado com o apoio de equipas de investigadores da Alemanha (responsável pela coordenação), Portugal, Espanha, Reino Unido, Irlanda e ainda por especialistas em tecnologias de informação e comunicação e cultura digital da Bulgária, Suíça e Noruega.

Este projeto originou um manual de formação sobre *ciber-bullying*, dirigido, em particular, a profissionais que trabalham este tema com diferentes públicos-alvo, especialmente jovens, famílias e escolas. Para além de incluir uma componente teórica, este manual oferece ainda orientações, apoio e recursos que pretendem contribuir para a prevenção e o combate a este problema (Matos et al., 2011).

4.5. Prevenção dirigida a grupos vulneráveis: o caso das crianças e jovens

Enquanto nativos das TIC, as crianças e jovens demonstram um **interesse e um gosto quase que naturais pelas atividades *online***. Sendo esta característica vantajosa em muitos domínios, também aumenta a **vulnerabilidade deste grupo ao envolvimento no cibercrime**, tanto no que se refere à cibervitimação, como no que respeita à perpetração (Alkan & Citak, 2007 *cit in* Edirisuriya & Liyanage, 2016).

Para este grupo, a comunicação através de ferramentas de comunicação suportadas pela Internet e as comunidades virtuais não são subculturas tecnológicas, mas antes formas de se manterem em contacto com os pares. A comunicação através destes meios parece ser privilegiada por esta população, por proporcionar maior sensação de privacidade e anonimato, favorecendo a desinibição, em detrimento da comunicação face-a-face (Chisholm, 2014).

Por se movimentarem de forma natural através da Internet e das TIC, não é incomum o envolvimento dos/as jovens em atividades ilícitas *online*, seja pela procura de sensações, por diversão ou por não associarem aos seus comportamentos eventuais consequências negativas. Veja-se a *PRÁTICA EM FOCO* sintetizada anteriormente – campanha de sensibilização desenvolvida pela EUROPOL *Cyber crime vs cyber security: what will you choose*? – que informa e alerta para as consequências do envolvimento em atividades *online* ilícitas e, pelo contrário, procura promover a adoção de condutas positivas e normativas.

De igual forma, o risco de cibervitimação é também maior entre a população mais jovem. Veja-se as *ESTATÍSTICAS EM FOCO* apresentadas em diversos pontos do capítulo 1 da parte I deste Manual.

4. A IMPORTÂNCIA DA PREVENÇÃO NO COMBATE AO CIBERCRIME

DESTAQUE | PRÁTICAS EM FOCO:

A EUROPOL disponibiliza, em *YOUR LIFE IS ONLINE. PROTECT IT!*, no seguimento da já referida campanha de sensibilização pública sobre extorsão sexual *online*, informação diversa para jovens, com o objetivo de reduzir o risco associado aos seus comportamentos *online* e níveis de exposição.

Contemplando informação sobre medidas de cibersegurança a adotar e que incrementam os **níveis de privacidade da presença digital**, nomeadamente nas redes sociais, a informação disponibilizada aborda ainda outros comportamentos pessoais de proteção que diminuem o risco de cibervitimação.

Veja-se https://www.europol.europa.eu/how-to-set-your-privacy-settings-social-media.

Adicionalmente, em *YOUR LIFE IS ONLINE. PROTECT IT!*, é ainda fornecida informação e instruções de atuação perante situações de cibervitimação, nomeadamente:

- Como solicitar a remoção de conteúdos em diferentes plataformas, em caso de divulgação não consensual de imagens e vídeos: https://www.europol.europa.eu/removing-links-to-explicit-content;
- Como pedir ajuda e denunciar, em situações de cibervitimação: https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/are-you-victim-get-help-report-it-we-are-here.

4.6. A prevenção situacional do cibercrime: uma questão de oportunidade

A **prevenção situacional do crime** surge enquanto paradigma teórico que se concentra nas circunstâncias associadas às oportunidades criminais e como o ambiente, as condições e o contexto podem ser modificados para impedir a sua manifestação. Este paradigma associa-se à Teoria da Escolha Racional e à Teoria das Atividades de Rotina[125] (Hinduja & Kooi, 2013):

- A escolha racional opera num nível micro, assumindo que o comportamento criminoso é impulsionado por algum tipo de objetivo que, em última análise, leva a um benefício. Assim, eventuais mudanças na estrutura da oportunidade podem afetar as perceções de risco, esforço e recompensa.
- As atividades de rotina operam no nível macro, demonstrando que as mudanças na vida quotidiana alteram o movimento de alvos adequados para o crime, a probabilidade de ação por eventuais autores/as e os níveis de vigilância.

A prevenção situacional do crime introduz o potencial de mudanças nos ambientes onde o crime pode ocorrer, tornando esses mesmos ambientes menos atraentes para criminosos/as motivados/as. A prevenção do crime assenta, assim, na redução das oportunidades de os/as criminosos/as beneficiarem das vulnerabilidades, através da gestão, *design* e manipulação desse ambiente, isto é, **da criação de obstáculos no ambiente para reduzir a probabilidade de as oportunidades criminais serem aproveitadas**. Idealmente, esses esforços servirão para aumentar o risco e o esforço associados à atividade ilícita e para diminuir as recompensas

[125] As teorias criminológicas (e sua aplicação para a compreensão da cibercriminalidade) são abordadas no ponto 3.1. do capítulo 3 da parte I deste Manual.

decorrentes da execução bem-sucedida do crime. Se a presença e a atratividade das possibilidades criminais forem diminuídas, o resultado culminará numa redução do crime (Clarke, 1997*cit in* Hinduja & Kooi, 2013).

Ao longo de várias décadas surgiram diferentes propostas e medidas de intervenção específicas para os ambientes em que os crimes ocorrem, que receberam o nome de **técnicas de prevenção situacional**. O seu principal objetivo é reduzir a oportunidade de o crime ocorrer, modificando as condições ambientais. Foram estabelecidas 5 categorias de prevenção situacional e, em cada uma dessas categorias, podem ser aplicadas 5 técnicas específicas (Cornish & Clarke, 2003 *cit in* Agustina, 2015):

Categoria *Aumento do esforço*:

Se for aumentado o esforço para a prática de um determinado crime, talvez seja possível dissuadir o/a autor face à sua prática.

Esta categoria integra 5 tipos de técnicas:

- endurecimento do alvo (implementação de barreiras que dificultam o acesso ao alvo);
- controlo de acessos (bloquear o acesso a locais em que a ação criminosa possa ocorrer);
- rastreio de saídas (controlo das saídas/movimentações de um certo *local*);
- desvio de autores/as (procura mudar os padrões de movimento de potenciais autores/as)
- controlo de instrumentos (limitar o acesso a instrumentos que façam parte do *modus operandi*).

Categoria *Aumento dos riscos*:

Estas técnicas destinam-se a aumentar o risco de o/a autor/a do crime ser detetado e incluem:

- aumento das atividades protetoras (criar atividades para que as pessoas se sintam mais protegidas; por exemplo, o *neighborhood watch*);
- assistência à vigilância natural (por exemplo, através do aumento da visibilidade de um dado *local*);
- redução do anonimato;
- vigilância informal (por exemplo, através da maior circulação de funcionários/a num espaço de comércio);
- vigilância formal (por exemplo, através de maior policiamento).

Categoria *Redução das recompensas*:

Nesta categoria, pretende-se reduzir as recompensas de que potenciais autores/as possam beneficiar com a prática de um crime.

As principais técnicas são:

- esconder alvos (por exemplo, estacionar em garagem privada, ao invés de estacionar em

local/via pública);
- remoção dos alvos (por exemplo, remover aparelhos eletrónicos e outros bens, ao estacionar o automóvel);
- identificar a propriedade (por exemplo, registo de propriedade automóvel);
- dificultar as transações de mercado (por exemplo, licenciamento de serviços e comércios);
- negar os benefícios (por exemplo, colocação de *password* no telemóvel).

Categoria *Redução das provocações*:

Esta categoria visa prevenir aspetos que desencadeiem a prática criminal.

As principais técnicas são:

- redução da frustração e *stress* (por exemplo, informar sobre saber o tempo de espera de um transporte público);
- evitar as disputas (por exemplo, separar claques desportivas em jogos de futebol/no desporto);
- redução da ativação emocional (por exemplo, controlar a visualização de violência que é transmitida nos *media*);
- neutralização da pressão dos pares (por exemplo, campanhas de sensibilização);
- desencorajamento da imitação (por exemplo, manutenção dos espaços limpos e cuidados ou remoção rápida de indicadores de vandalismo).

Categoria *Remoção de desculpas*:

Inclui as seguintes técnicas de prevenção situacional:

- definição de regras;
- afixação de instruções (por exemplo, sinalizações como "proibido estacionar");
- alertar à consciência (por exemplo, consciencializar para a ilegalidade da conduta);
- ajudar à conformidade (por exemplo, em eventos festivos, facilitar o acesso a meios públicos de transporte);
- controlo de álcool e drogas (por exemplo, imposição de número limite máximo de bebidas em estabelecimentos noturnos).

As abordagens de prevenção situacional foram amplamente utilizadas em contextos *tradicionais*, tendo-se revelado úteis na redução de diferentes tipos de crime *tradicionais*. Procurou-se igualmente analisar a relevância da prevenção situacional no combate ao cibercrime (Brewer et al., 2019).

Nesse contexto, Miró Llinares (2012, *cit in* Agustina, 2015) apresentou uma combinação de **medidas concretas para a prevenção situacional da cibercriminalidade**:

Quadro II-17: Técnicas de prevenção situacional aplicadas ao cibercrime

Redução do ambiente de incidência	Aumento do esforço percebido	Aumento do risco percebido	Redução de recompensas percebidas	Eliminação de desculpas
Não introdução de metas	Controlo de acesso ao sistema	Extensão da tutela/ vigilância	Ocultação de alvos	Estabelecimento de regras
Identificação de zonas de risco	Deteção e impedimento do ataque	Redução do anonimato	Remoção de alvos	Definição de regras
Descontaminação/ limpeza de resíduos	Desvio de autores/as	Fortalecimento da vigilância formal	Remoção de benefícios	Fortalecimento da consciência moral
Separação de alvos	Ferramentas/armas de controlo	Auxílio à vigilância natural	Interrupção de mercados	Assistência à conformidade

Foram 5 as categorias desenvolvidas - redução do ambiente de incidência; aumento do esforço percebido; aumento do risco percebido; redução de recompensas percebidas; eliminação de desculpas -, sendo 20 as técnicas de prevenção situacional do cibercrime. Em *redução do ambiente de incidência*, incluem-se a não introdução de metas (por exemplo, não acesso a *chats*), a identificação de zonas de risco (por exemplo, campanhas de informação sobre riscos nas redes sociais), a descontaminação/limpeza de resíduos e separação de alvos (por exemplo, criação de sub-redes de segurança local). Em *aumento do esforço percebido*, encontram-se: controlar acesso ao sistema (por exemplo, atualizar sistemas operativos e palavras-passes e licenças); detetar e impedir o ataque (por exemplo, antivírus; *anti-spyware; anti-spam*); desviar autores/as (por exemplo, remoção de conteúdo ilícito; negação de acesso a endereços de IP [126] específicos); ferramentas/armas de controlo. Em aumento do risco percebido são mencionadas a extensão da tutela/vigilância (por exemplo, denúncia por terceiros), a redução do anonimato (por exemplo, identificar endereços de IP; registo em fóruns da web; sistemas de identificação de utilizadores/as), o fortalecimento da vigilância formal (por exemplo, equipas especializadas em investigação do cibercrime) e o auxílio à vigilância natural (por exemplo, melhorar os sistemas de identificação de IP). A quarta categoria, por sua vez, foca-se em: ocultar alvos (por exemplo, usar sistemas de criptografia; ocultar dados pessoais nas redes sociais); remover alvos (por exemplo, utilizar discos rígidos removíveis; optar por sistemas de pagamento alternativos, como *PayPal*; não aceitar mensagens de pessoas desconhecidas); remover benefícios; interromper mercados (por exemplo, controlar *websites* de *download* direto de arquivos). Por fim, em *eliminação de desculpas* inclui-se: o estabelecimento de regras (por exemplo, harmonização jurídica internacional); a definição de regras (por exemplo, notificações de privacidade nas redes sociais); fortalecimento da consciência moral (por exemplo, aumentar a sensibilização sobre propriedade intelectual); e assistência à conformidade (por exemplo, competições legais de *hackers*; privilegiar o *software* aberto).

[126] IP diz respeito a endereço de protocolo de Internet e refere-se ao rótulo/código atribuído a cada dispositivo conectado a rede de computadores.

4. A IMPORTÂNCIA DA PREVENÇÃO NO COMBATE AO CIBERCRIME

As evidências disponíveis sobre a eficácia das técnicas de prevenção situacional do cibercrime têm estado centradas no aumento do esforço, como é o caso de mecanismos/*software* de controlo e deteção, e no aumento do risco, através de ferramentas formais de vigilância. A título exemplificativo, a investigação sobre a eficácia dos produtos antivírus na deteção e prevenção de infeções por *malware* revela que a maioria dos produtos é eficaz na deteção e prevenção desse tipo de infeções (Brewer et al., 2019).

[1] PORDATA, Indicadores de Envelhecimento, Índice de Envelhecimento 2018 https://www.pordata.pt/Portugal/Indicadores+de+envelhecimento-526 (consultado a 26-02-2020)

[2] Conselho Nacional de Ética para as Ciências da Vida, "Parecer 80/CNECV/2014 sobre as vulnerabilidades das pessoas idosas, em especial das que residem em instituições" (2014) https://www.cnecv.pt/admin/files/data/docs/1413212959_Parecer%2080%20CNECV%202014%20Aprovado%20FINAL.pdf (consultado a 27-02-2020)

BIBLIOGRAFIA
WEBGRAFIA

BIBLIOGRAFIA WEBGRAFIA

BIBLIOGRAFIA

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.

BIBLIOGRAFIA

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.

BIBLIOGRAFIA

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.

BIBLIOGRAFIA

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).

WEBGRAFIA

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=199&tabela=leis

http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=775&tabela=leis

https://apav.pt/cibercrime/

https://articles.forensicfocus.com/2019/12/17/investigating-nonconsensual-intimate-image-sharing/

https://data.consilium.europa.eu/doc/document/ST-7159-2017-REV-1-COR-1-DCL-1/en/pdf

https://dre.pt/legislacao-consolidada/-/lc/34520775/view

https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/criminal_code_germany_en_1.pdf

https://techterms.com/definition/hardware

https://www.cncs.gov.pt/recursos/glossario/

https://www.gesetze-im-internet.de/bdsg_2018/BJNR209710017.html

https://www.gesetze-im-internet.de/tkg_2004/

https://www.gesetze-im-internet.de/tmg/BJNR017910007.html

https://www.innocentlivesfoundation.org/gaming-and-grooming-how-minecraft-and-fortnite-could-be-dangerous/

https://www.kaspersky.com/blog/online-dating-report/

https://www.met.police.uk/advice/advice-and-information/fa/fraud/personal-fraud/online-shopping/

https://www.scamwatch.gov.au/types-of-scams/dating-romance

ROAR
empoderamento às vítimas de cibercrime

APAV
associação portuguesa de Apoio à Vítima

Este manual foi financiado pelo Fundo para a Segurança Interna – Polícia da União Europeia

MINISTÉRIO PÚBLICO
PORTUGAL
PROCURADORIA-GERAL DA REPÚBLICA

WEISSER RING
Wir helfen Kriminalitätsopfern.

ACTEDO

altice

ISBN:
978-989-54855-3-6