Instituto Superior de Ciências Policiais e Segurança Interna

Sara Margarida Teófilo Pereira

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

Cibersegurança:

o Papel da Polícia de Segurança Pública na Prevenção do Cibercrime

Orientadora:

Prof. Doutora Paula do Espírito Santo

Lisboa, 13 de maio de 2022

Instituto Superior de Ciências Policiais e Segurança Interna

Sara Margarida Teófilo Pereira

Aspirante a Oficial de Polícia

Dissertação de Mestrado Integrado em Ciências Policiais

XXXIV Curso de Formação de Oficiais de Polícia

Cibersegurança:

o Papel da Polícia de Segurança Pública na Prevenção do Cibercrime

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Ciências Policiais, elaborada sob a orientação da Prof.ª Doutora Paula do Espírito Santo.

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXIV CFOP
Orientadora:	Professora Doutora Paula do Espírito Santo
Título:	Cibersegurança: o Papel da Polícia de Segurança Pública na Prevenção do Cibercrime
Autor:	Sara Margarida Teófilo Pereira
Local de Edição:	Lisboa
Data de Edição:	maio de 2022

Dedicatória

Aos meus pais e aos meus irmãos.

Agradecimentos

Primeiramente agradeço o apoio e a força incondicional da minha família: os meus pais e os meus irmãos. Sem eles, não teria alcançado este feito. Os meus pais, Gina e Ricardo, pela confiança que sempre depositaram em mim e por acreditarem em mim, quando eu própria não o fazia. Sou o que sou graças a vocês e nunca vou conseguir retribuir tudo o que já fizeram e continuam a fazer por mim e pelos meus irmãos. Irei sempre recordar os ensinamentos e a ajuda constante do meu pai e a força de viver e pensamento positivo da minha mãe. A minha irmã Sofia, que esteve sempre ao meu lado, desde os treinos no estádio para as provas físicas, até à realização da Dissertação de Mestrado. O Ricardo, meu irmão, que só de saber que estava feliz me dava força para continuar, obrigada por me fazeres rir e por me teres ensinado o verdadeiro significado de amar. Só nós sabemos a dificuldade da caminhada, mas no final terá um gosto ainda mais saboroso.

Em segundo lugar gostaria de agradecer aos meus amigos que nunca deixaram de me motivar, em especial às três companheiras que fizeram parte do meu percurso no ISCPSI, com a certeza de que continuarão na minha vida. Como não poderia deixar de referir, um obrigado sentido ao Instituto Superior de Ciências Policiais e Segurança Interna, aos seus docentes, Oficiais, Chefes, Agentes e pessoal de apoio, pela aprendizagem e valores incutidos, reforçando a minha forma de ser e de estar, que foi sempre a mesma e da qual tenho muito orgulho. Aos meus colegas do 34.º Curso de Formação de Oficiais de Polícia pelo espírito de entreajuda, camaradagem, união e amizade, pelos momentos irrepetíveis e memoráveis, pelas palavras bonitas e motivacionais que sempre recebi. Ao meu Cabo-Verdiano preferido pelas longas conversas e gargalhadas que me proporcionou. À minha "avó" do Instituto pela cumplicidade e por ter tornado o primeiro ano desta aventura muito mais fácil e feliz. À Professora Doutora Paula do Espírito Santo pelos inúmeros conselhos, ajuda, disponibilidade e acima de tudo pela motivação e palavras de incentivo. A todos os digníssimos informadores qualificados e aos encarregados de educação pela colaboração neste estudo.

Para terminar, sou muito grata pelas vivências que o estágio me proporcionou, quer na 18ª quer na 71ª Esquadras, particularmente pelas pessoas, que sem saber me ensinaram muito. A todos os que privaram comigo, o meu eterno agradecimento. Porque a verdadeira essência de um momento está nas pessoas que connosco o partilham. Como bem eternizou Antoine de Saint-Exupéry: "aqueles que passam por nós, não vão sós, não nos deixam sós. Deixam um pouco de si, levam um pouco de nós" .

Resumo

O ciberespaço, com as suas particularidades e podendo ser acedido por qualquer pessoa, necessita de ser um local seguro para se tirar o melhor partido das potencialidades que tem para oferecer. A cibersegurança deve ser assegurada por cada pessoa que navega na *internet* e por quem pode contribuir para a prevenção da cibercriminalidade. Existem fatores de risco potenciadores da cibervitimação, mormente no que respeita à vulnerabilidade das crianças, idosos, adultos isolados, pessoas com perturbação mental, ou cujo comportamento sistemático favorece o ataque e o aproveitamento de alguém mal-intencionado. Para além disso, os cibercriminosos aproveitam-se da falta de segurança dos sistemas, da capacidade de anonimato e da iliteracia digital das pessoas.

A principal forma de prevenir o cibercrime é pela via da cibereducação e sensibilização, por parte das Polícias, sendo que este estudo irá debruçar-se sobre o papel da PSP na prevenção ao cibercrime. Em concreto, nesta investigação, examinam-se as vertentes de intervenção da PSP na prevenção do cibercrime – formação, sensibilização, colaboração, cooperação internacional e investigação criminal – e investigam-se os moldes da existência de ciberpoliciamento, por parte desta Polícia. Relativamente ao público-alvo mais novo – as crianças entre os 6 e os 10 anos -, o estudo demonstra que, apesar de os encarregados de educação relatarem que estas não passam largas horas sozinhas na *internet*, é possível, ainda assim, potenciar-se a criação de uma dependência dos ecrãs e a exposição ao risco. Os pais, de acordo com este estudo, tendem a apresentar pouca preocupação e cuidado, em relação à exposição dos filhos em matéria de cibercrime. A PSP tem apostado no policiamento de proximidade, com as EPES e EPAV, e no Núcleo de Cibercriminalidade, na prevenção e combate ao cibercrime, sendo que este estudo permite identificar os moldes e o papel da PSP nestes domínios.

Palavras-chave: Cibercrime; Ciberespaço; Cibersegurança; Cibervitimação; Prevenção.

Abstract

Cyberspace, with its characteristics and being accessed by anyone, needs to be a safe place to make the most of its potential. Cyber safety should be guaranteed by each person who surfs the *internet* and by those who can contribute for the prevention of cybercrime. There are certain risk factors enhancer of cyber victimization, mainly concerning the vulnerability of children, seniors, isolated adults, people with mental disorders, or whose systematic behaviour favors the attack and abuse from someone malicious. In addition, cyber criminals take advantage of the lack of security of the systems, the capacity for anonymity and people's digital illiteracy.

The main way of preventing cybercrime is through cyber education and awareness, from the Police forces, thus this study will focus on the role of PSP in the prevention of cyber crime. Specifically, this research aims to analyse the possibilities of PSP intervention int the prevention of cyber crime – training, awareness, collaboration, international cooperation and criminal investigation - and to investigate the possible ways of cyber policing from this Police force. In relation to the youngest target group - children between 6 and 10 years of age - this research shows that, in spite of the fact that parents say that children don't spend long hours in the *internet* by themselves, it is possible, even so, to potenciate an addiction to screens and an exposure to risk. Parents, according to this study, tend to reveal little concern and care, in relation to the exposure of children to cybercrime. PSP has invested in proximity policing, with EPES and EPAV, and at Cyber Criminality Department, in prevention and fighting cybercrime. This study makes it possible to identify the ways and the role of the PSP in these areas.

Keywords: Cybercrime; Cyber Safety; Cyberspace; Cyber Victimization; Prevention.

Lista de siglas e abreviaturas

Al.	Alínea
APA	American Psychological Association
APAV	Associação Portuguesa de Apoio à Vítima
APP	Aplicação digital
Art. º	Artigo
CERT.PT	Equipa de Resposta a Incidentes de Segurança Informática Nacional
CIS	Centro *Internet* Segura
CISA	Cybersecurity and Infrastructure Security Agency
CNCS	Centro Nacional de Cibersegurança
CRC	Committee on the Rights of the Child
DIP	Departamento de Informações Policiais
DIREST	Diretiva Estratégica
DN/PSP	Direção Nacional da Polícia de Segurança Pública
EC3	European CyberCrime Centre
EE	Encarregado de Educação
ENISA	European Union Agency for Cybersecurity
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EPAV	Equipas de Proximidade e de Apoio à Vítima
EPES	Equipas do Programa Escola Segura
EUA	Estados Unidos da América
EUROPOL	European Union Agency for Law Enforcement Cooperation
FBI	Federal Bureau of Investigation
GNR	Guarda Nacional Republicana
IC	Investigação Criminal
Inf	Informador Qualificado
INTERPOL	International Criminal Police Organization
IP	*Internet* Protocol

ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
LGBTQIA+	Lésbicas, gays, bissexuais, transexuais ou transgéneros, queer, intersexo, assexual, mais todas as diversas possibilidades de orientação sexual e/ou de identidade de género
MEO	MEO- Serviços de Comunicações e Multimédia
MIPP	Modelo Integrado de Policiamento de Proximidade
N. º	Número
NAOP	Núcleo de Apoio Operacional
NCiber	Núcleo de Cibercriminalidade
PJ	Polícia Judiciária
PP	Policiamento de Proximidade
PSP	Polícia de Segurança Pública
SICAD	Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
UK	United Kingdom
UMAR	União de Mulheres Alternativa e Resposta
UNICEF	United Nations International Children´s Emergency Fund
UPI	Uso Problemático da *Internet*

Índice

Dedicatória i
Agradecimentos ii
Resumo iii
Abstract iv
Lista de siglas e abreviaturas v
Índice de Apêndices ix
Índice de Quadros x
Índice de Gráficos xiii
Introdução 1
Capítulo 1: Enquadramento teórico-conceitual: cibersegurança e cibercrime 4
1.1. Conceito de cibersegurança, ciberespaço e cibercriminalidade 4
1.2. Evolução da cibercriminalidade no contexto ocidental entre os séculos XX e XXI 6
1.3. Caracterização do ciberespaço, ofensores e vítimas 8
1.4. Pilares da segurança interna 12
1.5. Modelos de policiamento 13
1.6. Modelo integrado de policiamento de proximidade na PSP 14
Capítulo 2: Vertentes de intervenção da PSP na prevenção de ilícitos no ciberespaço 20
2.1. Formação 20
2.2. Sensibilização 20
2.3. Colaboração nacional sobre cibersegurança e cibercrime 24
2.4. Cooperação internacional 24
2.5. Investigação criminal 26
Capítulo 3: Vitimação (cibernética) das crianças e jovens 27
3.1. *Cyberbullying* 28
3.2. Pornografia infantil 30
3.3. Ciberabuso nas relações de intimidade 32
3.4. *Cyberstalking* 34
3.5. Dependência *online* 35
3.6. Consequências da cibervitimação em crianças e jovens 36
3.7. A cibereducação como medida preventiva no combate ao cibercrime 37

Capítulo 4: Opções metodológicas e resultados 39
4.1. Opções metodológicas 39
4.2. Trabalho empírico: instrumentos de recolha de dados 41
4.3. Apresentação de resultados 44
4.4. Discussão de resultados 56
Conclusão 63
Referências 66
Apêndices 79

Índice de Apêndices

Apêndice A- Autorização para acesso a informação 79
Apêndice B- Termos de consentimento informado dos informadores qualificados 80
Apêndice C- Autorização para a realização das entrevistas 86
Apêndice D- Autorização da Direção do Agrupamento de Escolas Marcelino Mesquita .. 87
Apêndice E- Autorização da Direção do Agrupamento de Escolas Moinhos da Arroja 88
Apêndice F- Guião da entrevista 89
Apêndice G- Transcrições das entrevistas 90
Apêndice H- Questionário aplicado aos encarregados de educação de crianças a frequentar o 1º ciclo da Escola José Tagarro no Cartaxo e na Escola Manuel Coco em Odivelas 110
Apêndice I- Grelhas de análise de conteúdo das entrevistas realizadas aos polícias da PSP 114
Apêndice J- Análise estatística 138

Índice de Quadros

CORPO DO TEXTO

Quadro 1- Categorização da questão n.º1: "No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?" 45
Quadro 2- Categorização da questão n.º6 "Em relação ao MIIP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?" 48
Quadro 3- Frequência com que a criança pratica estas atividades nos tempos livres, por habilitações dos EE 53
Quadro 4- Frequência com que o EE encoraja a criança a explorar na *internet*, por habilitação literária 55
Quadro 5- Teste qui-quadrado das variáveis frequência com que o EE encoraja a criança a explorar na *internet* e habilitações literárias 55

APÊNDICES

Quadro 1- Matriz cromática das unidades de contexto e de registo da questão n.º 1 114
Quadro 2- Categorização da questão n.º1: "No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?" 116
Quadro 3- Matriz cromática das unidades de contexto e de registo da questão n.º 2 117
Quadro 4- Categorização da questão n.º2 "Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?" 118
Quadro 5- Matriz cromática das unidades de contexto e de registo da questão n.º 3 119
Quadro 6- Categorização da questão n.º3 "Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?" 121
Quadro 7- Matriz cromática das unidades de contexto e de registo da questão n.º 4 122
Quadro 8- Categorização da questão n.º4 "Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?" 124
Quadro 9- Matriz cromática das unidades de contexto e de registo da questão n.º 5 125
Quadro 10- Categorização da questão n.º5 "Quanto controlo *online* é necessário e quando é demasiado?" 126
Quadro 11- Matriz cromática das unidades de contexto e de registo da questão n.º 6 127
Quadro 12- Categorização da questão n.º6 "Em relação ao MIIP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?" 129
Quadro 13- Matriz cromática das unidades de contexto e de registo da questão n.º 7 130
Quadro 14- Categorização da questão n.º7 "Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique." 131
Quadro 15- Matriz cromática das unidades de contexto e de registo da questão n.º 8 132
Quadro 16- Categorização da questão n.º8 "Quais os riscos que correm as crianças ao navegar na *internet*?" 134
Quadro 17- Matriz cromática das unidades de contexto e de registo da questão n.º 9 135
Quadro 18- Categorização da questão n.º9 "Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar? 137
Quadro 19- Idade da criança 138
Quadro 20- Sexo da criança 138
Quadro 21- Ano de escolaridade da criança 138

Quadro 22- Habilitações literárias dos EE 139
Quadro 23- Apuramentos simples da variável "Frequência com que a criança está online no telemóvel, computador/portátil, *tablet* e consola" 139
Quadro 24- Apuramentos simples da variável " quanto tempo a criança costuma estar sozinha na *internet* num dia de semana" 140
Quadro 25- Apuramentos simples da variável "Tempo que a criança passa sozinha na *internet* num dia de fim de semana" 140
Quadro 26- Apuramentos simples da variável "Atividades que a criança mais pratica nos tempos livres" 141
Quadro 27- Apuramentos simples da variável "Atividades que a criança mais pratica nos tempos livres" 141
Quadro 28- Apuramentos simples da variável "Alterações Comportamentais da criança após a exposição às TIC" 142
Quadro 29- Apuramentos simples da variável "Alterações Comportamentais da criança após a exposição às TIC" 142
Quadro 30- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses" 143
Quadro 31- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses" 144
Quadro 32- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses" 145
Quadro 33- Apuramentos simples da variável "Ação tomada pelo EE relativamente à situação que aconteceu com a criança" 146
Quadro 34- Apuramentos simples da variável "Ação tomada pelo EE relativamente à situação que aconteceu com a criança" 146
Quadro 35- Apuramentos simples da variável "Cuidados do EE no acesso da criança à *internet*" 146
Quadro 36- Apuramentos simples da variável "Cuidados do EE no acesso da criança à *internet*" 147
Quadro 37- Apuramentos simples da variável "Frequência com que o EE encoraja, sugere, fala e ajuda a criança quando esta está *online*" 147
Quadro 38- Apuramentos simples da variável "Situações que aconteceram com a criança e o EE nos últimos doze meses" 148
Quadro 39- Apuramentos simples da variável " Situações que aconteceram com a criança e o EE nos últimos doze meses" 148
Quadro 40- Apuramentos simples da variável "Medidas a serem concretizadas na escola" 149
Quadro 41- Apuramentos simples da variável "Medidas a serem concretizadas na escola" 149
Quadro 42- Apuramentos simples da variável "Medidas a serem concretizadas na escola" 150
Quadro 43- Frequência em telemóvel, por idade da criança 151
Quadro 44- Teste qui-quadrado das variáveis frequência em telemóvel e idade 152
Quadro 45- Frequência em computador, por idade da criança 152
Quadro 46- Teste qui-quadrado das variáveis frequência em computador e idade 153
Quadro 47- Frequência em *tablet*, por idade da criança 153
Quadro 48- Teste qui-quadrado das variáveis frequência em *tablet* e idade 154
Quadro 49- Frequência em consola, por idade da criança 154
Quadro 50- Teste qui-quadrado das variáveis frequência em consola e idade 155
Quadro 51- Tempo que a criança fica sozinha na *internet* num dia de semana, por idade 158

Quadro 52- Tempo que a criança fica sozinha na *internet* num dia de fim de semana, por idade 159
Quadro 53- Frequência com que a criança convive *online*, por idade 160
Quadro 54- Frequência com que a criança convive *online*, por sexo 160
Quadro 55- Frequência com que a criança convive cara a cara, por sexo 161
Quadro 56- Frequência com que a criança pratica desporto ou outras atividades físicas, por sexo 161
Quadro 57- Frequência com que a criança joga videojogos, por sexo 161
Quadro 58- Frequência com que a criança faz atividades ao ar livre, por sexo 162
Quadro 59- Frequência com que a criança ajuda a família, por sexo 162
Quadro 60- Frequência com que a criança faz os TPC ou outras atividades escolares, por sexo 163
Quadro 61- Frequência com que a criança fica aborrecida por não estar nos dispositivos digitais, por idade 164
Quadro 62- Cuidados do EE no acesso da criança à *internet*, por habilitações literárias.. 165
Quadro 63- Cuidados do EE no acesso da criança à *internet*, por idade da criança 166
Quadro 64- Frequência com que o EE encoraja a criança a explorar na *internet*, por habilitação literária 167
Quadro 65- Teste qui-quadrado das variáveis frequência com que o EE encoraja a criança a explorar na *internet* e habilitações literárias 168
Quadro 66- Frequência com que o EE sugere modos de usar a *internet* de forma segura, por habilitação literária 169
Quadro 67- Teste qui-quadrado das variáveis frequência com que o EE sugere modos de usar a *internet* de forma segura e habilitações literárias 169
Quadro 68- Frequência com que o EE fala com a criança sobre o que ela faz *online*, por habilitação literária 170
Quadro 69- Teste qui-quadrado das variáveis frequência com que o EE fala com a criança sobre o que ela faz *online* e habilitações literárias 171
Quadro 70- Frequência com que o EE ajuda a criança quando algo a aborrece na *internet*, por habilitação literária 171
Quadro 71- Teste qui-quadrado das variáveis frequência com que o EE ajuda a criança quando algo a aborrece na *internet* e habilitações literárias 172
Quadro 72- Comparação das escolas relativamente à ida da Escola Segura e ao leccionamento de aulas sobre os riscos da *internet* e sobre competências digitais 174
Quadro 73- Comparação das escolas relativamente às habilitações dos EE 174
Quadro 74- Comparação das escolas relativamente às medidas selecionadas pelos EE a implementar 175
Quadro 75- Comparação das escolas relativamente às atividades que as crianças mais praticam nos tempos livres 176

Índice de Gráficos

CORPO DO TEXTO

Gráfico 1- Idade da criança 51
Gráfico 2- Sexo da criança 51
Gráfico 3- Ano de escolaridade da criança 51
Gráfico 4- Habilitações literárias dos EE 51

APÊNDICES

Gráfico 5- Frequência em telemóvel, por sexo da criança 155
Gráfico 6- Frequência em computador, por sexo da criança 156
Gráfico 7- Frequência em tablet, por sexo da criança..... 156
Gráfico 8- Frequência em consola, por sexo da criança 157
Gráfico 9- Receber visita da Escola Segura, por ano de escolaridade..... 172
Gráfico 10- Ter aulas sobre os benefícios e riscos da *internet*, por ano de escolaridade... 173
Gráfico 11- Ter aulas de competências digitais, por ano de escolaridade 173

Introdução

A proliferação das tecnologias de informação e comunicação, a partir da década de 90, verificando-se atualmente um número muito elevado de pessoas (5 biliões) com acesso à *internet*, correspondendo a 63% da população mundial (Data Reportal, 2021), contribuiu para o aumento das ameaças e desafios cibernéticos. Assiste-se a uma contínua evolução e aperfeiçoamento de formas de levar a cabo ataques via *online*. Disso são exemplo as burlas, em Portugal, em especial durante o tempo de pandemia, na aplicação *mbway*.

A Teoria das Oportunidades sustenta que "existem ambientes mais propícios para o cometimento de crimes por causa do maior número de oportunidades que proporcionam" (Santos et al., 2008, p.37). Os infratores aproveitam-se das vulnerabilidades do meio e dos seus utilizadores, em especial a falta de segurança dos sistemas, do seu próprio anonimato e da iliteracia digital e inocência das pessoas. Estes três aspetos permitem ao ofensor fazer uma análise custo-benefício, apostando no cometimento do ilícito. A pandemia *Covid-19*, que teve início em fevereiro de 2019 e que se mantém ainda em finais de 2021 e início de 2022, potenciou uma oportunidade a aproveitar pelos ofensores, uma vez que durante os confinamentos, a utilização da *internet* e das TIC aumentou exponencialmente, conforme demonstram os estudos (EUROPOL, 2020a, 2020b e 2020c; INTERPOL, 2020a; Kemp et. al, 2021; Centro Nacional de Cibersegurança, 2020 e 2021a).

A investigação que se apresenta trata do tema referente à cibersegurança e ao cibercrime e ao ciberpoliciamento, que fazem parte das linhas de investigação do Centro de Investigação ICPOL do ISCPSI: Polícia e Sociedade e Policiamento, respetivamente. Adensa-se a sua pertinência por ser um dos eixos estratégicos para o biénio 2020-2022 da Direção Nacional da Polícia de Segurança Pública "reforçar a capacidade de investigar os crimes cometidos em ambiente digital e de ciberpoliciamento" (Direção Nacional, 2020, p.5). Em 2019, já tinha surgido a Resolução do Conselho de Ministros n.º 92/2019, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Pese que embora a investigação da criminalidade informática seja da competência reservada da Polícia Judiciária, conforme a Lei de Organização da Investigação Criminal (artigo 7. º, n. º3, al. l), da Lei n.º 49/2008, de 27 de agosto), esta matéria carece da responsabilidade e intervenção de vários atores, desde a Polícia e o Estado aos próprios cidadãos, pois só assim se poderá minimizar a ocorrência de ciberataques e preveni-los. Neste sentido, foi criado, em novembro de 2020, um Núcleo de Cibercriminalidade no Departamento de Investigação Criminal da Direção Nacional da PSP.

A segurança total é uma utopia, pelo que o caminho deve ser o da prevenção, por forma a antecipar comportamentos, reduzir a probabilidade de concretização dos ciberataques e minimizar as suas consequências. De acordo com a Teoria das Atividades Rotineiras, desenvolvida por Lawrence E. Cohen e Marcus Felson (1979), num contexto pandémico, seria expectável que estes crimes fossem aumentar abruptamente, pois existia um alvo vulnerável, um ambiente favorável à prática do crime e um infrator motivado. Acresce ainda a ausência de um "guardião" (Tilley, 2005) (inexistência de ciberpoliciamento). No entanto, houve um aumento significativo do número de incidentes de cibersegurança em Portugal a partir do mês de março de 2020, o início da resposta nacional à pandemia, de acordo com o *Relatório Cibersegurança em Portugal-Riscos e Conflitos 2020* (CNCS, 2020, p.80).

A prevenção criminal constitui um dos cinco pilares da Segurança Interna, sendo uma "função primordial em qualquer Estado de direito democrático" (Elias, 2018, p. 89). O mesmo autor refere que aquela deve ser aplicada aos três fatores anteriormente citados, minimizando a motivação do infrator, fortalecendo o alvo e eliminando as oportunidades que o meio propicia. O modelo de policiamento de proximidade, implementado pela Polícia de Segurança Pública, integra-se neste pilar, tendo como principais objetivos prevenir a criminalidade e diminuir o sentimento de insegurança dos cidadãos (David, 2014). Para além disso, o mesmo articula-se com as Informações e a Investigação Criminal, outras valências da PSP, essenciais neste âmbito da cibersegurança. Outro aspeto a considerar é o facto de ser um policiamento que busca a colaboração e a cooperação global da segurança.

O objeto de estudo irá centrar-se na cibersegurança, examinando-se as vertentes de atuação da PSP na prevenção do cibercrime, com enfoque no Policiamento de Proximidade. O problema de investigação traduz-se na interrogação: qual a atuação da PSP no que diz respeito ao cibercrime e à sua prevenção? Como tal, a pergunta de partida é a seguinte: De que forma a PSP pode contribuir para a cibersegurança e consequentemente prevenir o cibercrime? Desta questão surgem duas questões derivadas que são: quais são as áreas de intervenção da atuação preventiva da PSP? De que forma o ciberpoliciamento tem vindo a ser aprofundado?

No presente estudo tem-se como objetivo geral: examinar o papel da PSP na prevenção do cibercrime, identificando-se as várias vertentes de intervenção na prevenção destes ilícitos e aferir da existência de ciberpoliciamento nesta Polícia. Os objetivos específicos são: caracterizar o ciberespaço, os ofensores e as vítimas; examinar em que medida o Modelo Integrado de Policiamento de Proximidade está adaptado ao ciberespaço

e quais as suas principais valências, limitações e obstáculos; conhecer o grau de conhecimento por parte de encarregados de educação de crianças, entre os seis e os dez anos, em relação aos riscos que correm com a utilização dos meios tecnológicos e examinar o impacto da cibervitimação nas crianças e jovens.

Por forma a responder às questões e objetivos supra, para além da revisão da literatura no sentido de melhor compreender os fenómenos em estudo, serão realizadas entrevistas a informadores qualificados no campo da cibersegurança, da atuação policial e das vítimas e aplicado um inquérito por questionário a encarregados de educação de crianças dos seis aos dez anos, a frequentar o primeiro ciclo do Ensino Básico numa Escola no Cartaxo e noutra em Odivelas.

Quanto à estrutura da dissertação, esta contempla a introdução, três capítulos, resultados e conclusão. No primeiro capítulo, é feito um enquadramento teórico-conceitual acerca da cibersegurança, do ciberespaço e da cibercriminalidade, procurando, posteriormente, caracterizar o ciberespaço, os ofensores e as vítimas, tendo em consideração a evolução da cibercriminalidade entre os séculos XX e XXI no contexto democrático ocidental. São referidos os pilares da segurança interna, com enfoque na prevenção criminal e os modelos de policiamento, máxime o de proximidade. Além disso, dedica-se um subcapítulo ao MIPP e à sua adaptação ao ciberespaço, com o intuito de perceber quais as suas valências, limitações e obstáculos.

No segundo capítulo, será examinado o papel da PSP na segurança do ciberespaço, nas diversas vertentes de intervenção: formação, sensibilização, colaboração, cooperação internacional e investigação criminal.

No terceiro capítulo, optou-se por estudar um público-alvo específico, em que a PSP pode apostar, as crianças e jovens, no que se refere à vitimação, os principais crimes a que podem ser expostos, como o *cyberbullying*, a pornografia infantil, o ciberabuso nas relações de intimidade e o *cyberstalking*, a dependência das novas tecnologias e as consequências daí resultantes.

No quarto capítulo, são apresentadas as opções metodológicas e o trabalho empírico, procedendo-se ainda à análise e discussão dos resultados, com vista a responder às questões de investigação. Por fim, são expostas as principais conclusões, as limitações na realização deste estudo e ainda recomendadas linhas de investigação futuras.

Capítulo 1: Enquadramento teórico-conceitual: cibersegurança e cibercrime

1.1. Conceito de cibersegurança, ciberespaço e cibercriminalidade

A origem do conceito "cibersegurança" remonta ao ano de 1903 quando foi enviada uma mensagem insultuosa, pelo filósofo e engenheiro John Fleming, através de código morse, ao matemático e astrónomo Nevil Maskelyne (Thakur & Pathan, 2020). Em resposta aos ataques terroristas de 11 de setembro de 2001 e subsequentes envios de *anthrax* pelo correio foi criada uma das primeiras legislações contendo disposições acerca de cibersegurança (Kremling & Parker, 2018).

A *Estratégia Nacional de Segurança do Ciberespaço 2019-2023* define cibersegurança como:

> "O conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem". (Resolução do Conselho de Ministros, 2019)

Militão (2014, p. 26) defende que cibersegurança diz respeito às medidas que garantem o bem-estar das pessoas e o normal funcionamento das instituições democráticas no ciberespaço e fora dele. Segundo a *UK National Cyber Security Strategy*, cibersegurança pode ser descrita como sendo a proteção dos sistemas de informação (*hardware*, *software* e infraestruturas associadas), dos seus dados e dos serviços que prestam, contra o acesso não autorizado, danos ou utilização indevida (HM Government, 2016). Já nos Estados Unidos da América, a *Cybersecurity & Infrastructure Secure Agency* (CISA) refere que a: "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (CISA, 2019). O conceito adotado pelo Centro Nacional de Cibersegurança (2021b) vai ao encontro do da Estratégia anteriormente mencionado, acrescentando "o sentimento de segurança percecionado pelas pessoas quando usam a *internet* e as tecnologias digitais". Para a autora, a que se destaca é a do CNCS, pois o ativo mais importante aqui presente são as pessoas que, ao estar por detrás das máquinas, estão ligadas a qualquer problema ou em parte responsáveis pela sua prevenção e/ou solução (Singer & Friedman,

2014). Neste sentido, aquelas são também quem vai sofrer as consequências se o espaço digital não for seguro.

O ciberespaço é descrito na *Estratégia Nacional de Segurança do Ciberespaço 2019-2023* como sendo um ambiente complexo, da responsabilidade de todos, onde existe a interação entre pessoas, redes e sistemas de informação (Resolução do Conselho de Ministros, 2019). Trata-se, essencialmente, de um ambiente de informação, onde esta é criada/comunicada, guardada e partilhada (Singer & Friedman, 2014), por exemplo, onde se fazem negócios, se criam e desenvolvem relações ou se cria e se aprecia arte (Martin et al., 2019). Contudo, para além dos aspetos positivos, também possibilita uma vasta panóplia de crimes, cujos impactos são "virtuais" mas também físicos, pois além de poder afetar toda uma instalação (Martin et al., 2019; Thakur & Pathan, 2020), afeta consequentemente os utilizadores.

O cibercrime compreende os ilícitos criminais praticados com recurso a meios tecnológicos (Elias, 2018), através de um computador e pela *internet*, plataformas de redes sociais, correio eletrónico ou outro (Guedes et al., 2021), explorando o ciberespaço. Desta forma, um ciberataque é uma tentativa deliberada por parte de uma organização ou de um indivíduo para invadir o ambiente cibernético de outrem (s) com um objetivo específico, seja ele apagar, furtar ou danificar informação (Thakur & Pathan, 2020), ofender, divulgar conteúdos indecentes e ilícitos ou ainda infligir danos contra a propriedade (Guedes et al., 2021).

No âmbito da cibercriminalidade, como refere Ribeiro (2015), englobam-se quer os crimes ditos tradicionais, como a burla informática prevista no Código Penal (Art.º n.º 221.º) ou o acesso ilegítimo previsto na Lei do Cibercrime (Art.º n.º 6.º), quer os novos crimes informáticos, como a *sextortion* (extorsão de favores sexuais à vítima) e o *cyberbullying*. As formas de os cometer são também bastante variadas, existindo, na ótica de Robalo (2021), duas tipologias de cibercrime: os de baixa tecnologia e os de alta tecnologia, dependendo do alvo a atingir. Os primeiros não exigem grandes conhecimentos informáticos pois o alvo é a vítima em si mesma, contrariamente aos segundos, onde o alvo é o próprio sistema informático (Robalo, 2021). Existem várias outras categorias a subdividir estes crimes, mas não se considera relevante colocar, até porque "a single computer crime may actually entail a number of distinct offences" (Grabosky, 2015, p. 8).

Segundo a *McConnell International* (2000, pp. 1-2), o cibercrime difere do crime terrestre, pela facilidade com que é aprendido e interiorizado, a relação custo-benefício é positiva (poucos recursos podem causar um enorme dano), podem ser praticados numa

jurisdição sem o ofensor se encontrar lá fisicamente e muitas vezes não são claramente ilegais devido à sua territorialidade (Amador, 2018, pp. 19-20).

1.2. Evolução da cibercriminalidade no contexto ocidental entre os séculos XX e XXI

Os primeiros computadores foram criados nos anos 40 do século XX e possuíam vantagens em termos de segurança, pois eram de grandes dimensões, bastante dispendiosos e por conseguinte sistemas independentes (Cross, 2008). A proliferação dos computadores despoletou os riscos do *hacking,* aparecendo em 1961, nos EUA, o primeiro grupo de *hackers* chamado "Tech Model Railroad Club" (Cross, 2008). Posteriormente, com a criação do *e-mail,* no início dos anos de 1970, e com o surgimento do *World Wide Web* em 1990, foram surgindo novas formas de cibercrime, como os vírus, por exemplo o "Melissa", o "Nigerian letter" (Cross, 2008) ou o "I love you" no ano de 2000 (Grabosky, 2014).

No século XXI, devido à evolução da tecnologia digital, o cibercrime tornou-se mais sofisticado, corrente e inclusive comercializado, existindo hoje em dia na *internet* as ferramentas necessárias para perpetrar um ataque, seja comprando, seja fazendo *download* (Grabosky, 2014). Por outro lado, face a essa facilidade com que se adquirem os meios, cada vez mais os *hackers* não necessitam de possuir grandes competências informáticas para cometer um destes crimes e estes não são assim tão sofisticados. De 2000 a 2010, surgiu o *phishing*, as *BotNets*, a pornografia infantil ou o *hacktivismo*. Atualmente existem mais tipologias de cibercrime (e.g. ciberespionagem, *spam mobile device attacks, ransomware, social media manipulation, cyber warfare, banking malware, bitcoin wallet stealers, Covid-19 hackers targeted pharmaceutical companies/ spread desinformation)* e no futuro existirão outras porque o desenvolvimento tecnológico cria as oportunidades para a ofensa (Alexandrou, 2021).

O cenário do aumento do cibercrime verifica-se em contextos e países muito diferentes. Em 2014, o cibercrime custou quase 500 biliões de euros, tendo aumentado para 600 biliões em 2018. Mas "what about the nonfinancial costs to human suffering and freedom?" (Alexandrou, 2021, p.81).

O FBI (Federal Bureau of Investigation) registou um aumento de 300% de queixas relativas a ataques cibernéticos em abril de 2020 (Barrinha, 2020). No seu *Internet Crime Report* a Inglaterra, o Canadá, a Índia, a Grécia e a Austrália foram os países mais vítimas destes crimes em 2020. De acordo com um estudo feito pela Beaming UK (2020), entre 2015 e 2019, o cibercrime duplicou. Em Inglaterra e no País de Gales, o crime mais registado é a

fraude informática, com 3.8 milhões de incidentes em setembro de 2019, vitimando maioritariamente indivíduos com mais de 60 anos (National Crime Agency, 2020). No Relatório *The 2020 Data Attack Surface* está previsto que, até ao final desta década, 7.5 biliões de pessoas, ou seja, 90% da população mundial, vai ter acesso à *internet* e irá gerar dados, dados esses que chegarão aos 200 *zettabytes* até 2025 (Arcserve, 2020). Tal representa a quantidade de *data* que é necessário proteger do cibercrime (Stainer, 2021).

No plano nacional, entre 2009 e 2020, verifica-se um aumento constante no número de crimes informáticos, de crime de devassa por meio informático e de crime de burla informática/comunicações, de acordo com o *Relatório Riscos e Conflitos 2020* e a Direção-Geral da Política de Justiça (CNCS, 2020). A burla informática/comunicações foi o que apresentou o maior número de condenados (74% em 2018). Em 2020, apesar de a criminalidade em geral ter diminuído, o crime relacionado com a informática aumentou face a 2019, sendo o acesso/interceção ilegítimos o mais registado pelas autoridades policiais, segundo consta no *Relatório Riscos e Conflitos 2021* (CNCS, 2021a).

Em 2020, o Gabinete de Cibercrime, da Procuradoria Geral da República, registou mais denúncias (+183%) e a Linha Internet Segura abriu mais processos de atendimento e apoio (+41%) e registou mais 475% de crimes, em comparação com o ano anterior (CNCS, 2021b). A ameaça, a difamação/injúrias, a violência doméstica e a *sextortion* foram os crimes contra as pessoas mais registados pela APAV, através da citada Linha (CNCS, 2021b). Daqui retirou-se que a criminalidade mais denunciada é a defraudação na utilização da MBWAY, o *phishing* e o *ransomware*. De notar que o primeiro, ao contrário dos outros dois, que surgiram na década de 90 e 80 respetivamente, é recente, um aproveitamento da afluência à referida aplicação. O *phishing/smishing* e o sistema infetado por *malware* foram os tipos de incidentes mais registados em 2019 e 2020. O Relatório afirma ainda que a tendência é a cibercriminalidade continuar elevada em 2022, sendo que permanecerá uma realidade. Em 2020 e 2021 aumentou a perceção de risco de se sofrer um incidente de cibersegurança no ciberespaço de interesse nacional (CNCS, 2021b). Ressalvar que o serviço que coordena a resposta a incidentes de cibersegurança no ciberespaço português é o CERT.PT, integrado no Centro Nacional de Cibersegurança que, por sua vez, funciona no âmbito do Gabinete Nacional de Segurança, sendo a Autoridade Nacional de Cibersegurança. De referir ainda a ausência da PSP na composição do Conselho Superior de Segurança do Ciberespaço (cfr. Art.º 5.º da Lei n.º46/2018). De salientar que os dados referidos apuraram-se com base nas queixas apresentadas às autoridades, pelo que de fora ficam muitos outros incidentes que não são reportados, o que perfazia números muito mais

elevados, as chamadas "cifras negras". Na opinião de Amador (2018), poderá dever-se ao facto de as vítimas não darem importância à cibercriminalidade ou nem se aperceberem de que foram alvo ou por acreditarem ser impossível a identificação e punição dos infratores. De facto, o anonimato, as dinâmicas da rede, a volatilidade e o carácter temporário da prova digital (Santos et al., 2008) e o elemento da territorialidade (Amador, 2018) tornam difícil a investigação do crime informático. Por exemplo, se o crime for cometido em alto mar.

A pandemia contribuiu para a proliferação massiva de desinformação nas redes sociais e, concomitantemente, para a disseminação de campanhas de *phishing* (Santos, 2020). O *phishing* ocorre quando alguém, para conseguir obter informação pessoal de outrem, utiliza formas dissimuladas e enganadoras, como mensagens no correio eletrónico ou mensagens de *phishing*, com o intuito de levar a vítima a abrir anexos maliciosos, carregar em *URL´s* pouco seguros ou a transferir dinheiro (ENISA, 2018). Segundo Adam Kujawa, diretor do *Malwarebytes Labs*, esta abordagem é a forma mais fácil de cibercrime, uma vez que não explora as vulnerabilidades técnicas da *internet*, mas sim do seu utilizador e, por isso também a mais perigosa e eficaz (Malwarebytes, para. 3).

1.3. Caracterização do ciberespaço, ofensores e vítimas

O ciberespaço pode ser caracterizado como "um ecossistema de atores com interesses e capacidades específicas" (Singer & Friedman, 2014, p.178). Na ótica de Leukfeldt e Holt (2020), este espaço possui algumas especificidades como: ser ingovernável, ser impossível de policiar e estar mais além do que qualquer lei. No que toca à concretização do seu policiamento é algo que se irá verificar com a realização desta investigação. Adicionalmente, este confere uma variedade de oportunidades ao cibercrime, quer seja pela nova forma de explorar a distância, a ligação com as vítimas ou os ofensores assumirem identidades anónimas transitórias, dificultando em simultâneo a investigação destes ilícitos (Leukfeldt & Holt, 2020). O ciberespaço não é criado pelo computador mas sim pelas interconexões geradas (Clark, 2010). Podemos defini-lo através de quatro camadas: a primeira é a física, composta pelos dispositivos informáticos, pelo que é tangível e localizável; a segunda é a lógica, uma vez que as forças e as limitações do ciberespaço vêm das decisões que se fazem e de como são construídos os serviços, as aplicações, as plataformas, que estão sempre a evoluir; a camada da informação é central pois esta é aqui criada, armazenada e processada, adquirindo várias formas (música, vídeos, livros, fotografias, *websites*), podendo levantar questões de propriedade, autenticidade e fiabilidade à medida que mais informação entra

online; a camada do topo são as pessoas, que definem e moldam as características do ciberespaço através da forma como o utilizam (Clark, 2010). O autor afirma que os ataques podem vir de qualquer uma das camadas, por exemplo, desde destruir os componentes físicos até à corrupção das pessoas. Assim, torna-se importante compreendê-las para as poder proteger (Clark, 2010).

Miró-Llinares (2015) refere que os crimes perpetrados neste espaço estão estreitamente relacionados com o perfil do infrator e da vítima e a forma como o próprio crime é expresso é diferente dos crimes físicos. Pelo contrário, Leukfeldt e Holt (2020) argumentam que o cibercrime não está correlacionado com tipos específicos de ofensores/vítimas e que a sua caracterização tem sido um método incerto. Acredita-se que, como mencionado infra, existem certas características de pessoas que se inserem mais num tipo de crime, porém não é certo e vai se alterando espácio-temporalmente.

Não existe um "perfil" típico do cibercriminoso, nem da vítima, pois as suas características variam consoante o tipo de crime (Grabosky, 2015). Cada ofensor tem os seus objetivos, fazendo dele um *hacker*, um hacktivista, um burlão ou até um terrorista. Por exemplo, as motivações de um *hacker* podem ser: obter ganho monetário, prejudicar algo/alguém, infligir danos através do ciberterrorismo, adquirir informação reservada, realizar um ataque cibernético de guerra, entre outras (Thakur & Pathan, 2020). Além disso, alguns atuam somente por curiosidade e outros ainda por razões ideológicas. Estes últimos são os chamados *hacktivistas* e perpetuam ataques com a intenção de atingir determinadas causas (Kremling & Parker, 2018). Os ofensores estudam e identificam as vulnerabilidades quer dos sistemas, equipamentos ou das pessoas e posteriormente realizam os procedimentos tendentes aos seus objetivos (Antunes & Rodrigues, 2018). Ademais, as redes sociais são uma ferramenta que permite estabelecer relações virtuais, especialmente entre as pessoas mais jovens (Kremling & Parker, 2018), em que são gerados, comentados e partilhados conteúdos e expressadas emoções e opiniões sobre os mesmos (Antunes & Rodrigues, 2018). A par disso, os riscos que podem advir daí são enormes, uma vez que os utilizadores, muitas vezes, partilham informações pessoais ou vão ao encontro da pessoa por detrás do aparelho digital (Kremling & Parker, 2018). As consequências podem ser várias, como difamação, *sextortion*, *cyberbullying*, *cyberstalking*, pornografia infantil ou pode levar, no plano físico a rapto, sequestro, abuso sexual de menores, violação, etc. (Kremling & Parker, 2018). O anonimato que estas plataformas conferem aos infratores facilita o crime sexual (Kremling & Parker, 2018), permitindo-lhes entrar no mercado da pornografia infantil, da pedofilia ou fazerem-se passar por alguém para se encontrarem com a vítima. Não obstante, de vários

estudos feitos nos EUA, UK e Canadá, concluiu-se que a maior parte dos ofensores sexuais *online* eram caucasianos, ligeiramente mais jovens, desempregados, nunca estiveram casados e experienciaram mais episódios de violência física e sexual que a população em geral e que os ofensores sexuais "terrestres" (Grabosky, 2015).

Quando a *internet* foi introduzida os cibercriminosos eram maioritariamente jovens a viver com os pais e que desenvolviam vírus (*malware)* (Kremling & Parker, 2018). Segundo Kremling e Parker (2018), atualmente, os cibercriminosos são peritos informáticos sofisticados com uma idade média de 35 anos. Grabosky (2015) argumentava que os maiores *hackers*, indivíduos brilhantes eram a exceção e abaixo deles havia aqueles que descarregavam as ferramentas da *internet*, o mais comum, e ainda menos experientes estavam os indivíduos, aparentemente de países pouco desenvolvidos tecnologicamente, cujas ofertas fraudulentas indicavam e indicam um nível muito baixo de literacia.

As vítimas de cibercrime tendem a expor-se em demasia ao risco, ou seja, ao ofensor, nomeadamente, pelas horas que passam na *internet*. Por exemplo, ao envolverem-se em atividades interativas como compras *online*, as vítimas estão mais vulneráveis ao *phishing* ou fraude; ao estarem frequentemente nas redes sociais e em *chat rooms* ficam mais propícias ao *bullying* ou ao assédio (Grabosky, 2015). Outras atividades em que o utilizador se expõe a um ofensor motivado são por exemplo, utilizar o correio eletrónico, jogar jogos, ter um comportamento desviante e ainda possuir poucas competências de utilização da *internet* (Bossler & Holt, 2009; Ngo & Paternoster, 2011). Robalo (2021) defende que a teoria do estilo de vida representa uma justificação plausível para a cibervitimação no que toca aos cibercrimes de baixa tecnologia. Relativamente aos crimes de alta tecnologia, Choi (2008) acredita na aplicabilidade da teoria das atividades de rotina juntamente com a referida supra, pois a prática de certas condutas que acarretam riscos e a inexistência de elementos de proteção eficazes, levam a que uma pessoa seja vítima de um cibercrime.

Um estudo feito por Holt et al. (2014) concluiu que o risco de vitimação aumenta para aqueles que já experienciaram *bullying* fisicamente e ainda que as mulheres são mais suscetíveis de serem vitimadas. Williams (2015) através de inquéritos a 27 países europeus, aferiu que as pessoas com menos risco de vitimação são as que possuem um estatuto socioeconómico médio. Em relação ao *cyberstalking*, Nobles et al. (2014) descobriram que as vítimas *online*, em comparação com as terrestres, eram ligeiramente mais jovens, uma grande percentagem era caucasiana, do sexo masculino e detinham níveis de rendimento e educação superiores. Os estudos (Oksanen & Keipe, 2013; Hadlington & Chivers, 2018) têm demonstrado que os jovens são particularmente propensos à vitimação por cibercrime

(Guedes et al., 2021). No que concerne ao tráfico de pessoas, podem existir vários tipos de vítimas (Sykiotou, 2007): aquelas que procuram *sites* inofensivos mas que, direciona-as depois para outros potencialmente perigosos; as que usam *sites* potencialmente arriscados (*chats*, *sites* de namoro, *sites* de agências de casamento), sem se aperceberem dos riscos, talvez devido à idade e inocência; outras que usam *sites* perigosos conscientemente pensando que nada lhes poderá acontecer e ainda outras que, por desespero, aceitam ofertas de trabalho, sabendo que podem ficar em perigo (as cited in Cunha et al., 2021).

O estudo do medo do cibercrime, a par de conhecer o nível de suscetibilidade ao mesmo, é bastante importante para permitir a adaptação e direcionamento das estratégias de prevenção a grupos populacionais de maior risco ou mais suscetíveis ao cibercrime (Hadlington & Chivers, 2018). Relativamente ao género, as mulheres reportam níveis mais elevados de medo do que os homens (Al-Shalan, 2006; Yu, 2014; Virtanen, 2017; Martins, 2018); em relação à idade, não existem resultados únicos, apontando uns para os mais novos e outros para os mais velhos, mormente devido a estes últimos conferirem maior importância ao valor da propriedade e, consequentemente sentirem mais medo de a perder (Al-Shalan, 2006); as variáveis vitimação anterior, nível de educação e o nível de estatuto socioeconómico também apresentam resultados mistos (Guedes et al., 2021). Por último, o conhecimento informático está relacionado com o medo do crime (Virtanen, 2017; Martins, 2018), especialmente em crimes como o furto de identidade *online*, o *hacking* e a propagação de vírus informáticos, isto porque os indivíduos com menos conhecimento sentem-se mais vulneráveis e menos capazes para enfrentar eventuais danos (Guedes et al., 2021).

As vítimas, especialmente as de crimes sexuais, muitas vezes não denunciam para evitar mais vergonha e constrangimento. Estes ataques *online* podem causar às vítimas danos reais e materiais no mundo *offline* (Martellozzo & Jane, 2017).

Em suma, é importante ficar a conhecer melhor o ciberespaço e as pessoas que fazem parte dele, para se perceber de que forma se pode atuar para torná-lo num local mais seguro, quer seja ao nível dos sistemas, quer seja ao nível dos utilizadores. Sendo que este trabalho se inclina para o segundo, porque por detrás dos aparelhos estão pessoas que precisam de ser elucidadas dos riscos que correm e ensinadas a reforçar a proteção daqueles.

1.4. Pilares da segurança interna

Para a prossecução da sua missão, a atividade policial abrange um espetro de valências muito complexo, desde o policiamento de proximidade, passando pela ordem pública e a proteção do ambiente. Para garantir que todos os problemas criminais são resolvidos da melhor forma, as polícias integrais ("aquelas que têm um quadro holístico de competências legais, de valências e de capacidades, não necessariamente todas as possíveis") (Elias, 2018, p.87), possuem um conjunto variado de competências que se integram nos denominados pilares da segurança interna, sendo eles: a prevenção da criminalidade, a ordem pública, a investigação criminal, a inteligência ou informações policiais e a cooperação internacional (Elias, 2018). Neste trabalho importa aprofundar o primeiro, ou seja, a prevenção criminal.

1.4.1 Prevenção Criminal

A prevenção criminal engloba qualquer ação concebida para reduzir o nível de criminalidade e a gravidade das suas consequências (Ekblom, 2005) e/ou ainda a perceção do medo do crime (Fisher & Lab, 2010). Segundo Oliveira (2002, p.79), trata-se do "conjunto de medidas, cuja intenção é minimizar as infrações (a sua frequência, a sua gravidade e as suas consequências) ", pelo que uma ação de natureza preventiva tem por base a previsão e a intervenção precoce (Fernandes, 2006). Assim, a redução dos riscos e o reforço dos fatores de proteção levam à diminuição do crime e ao aumento do sentimento de segurança (Fernandes, 2006). A ideia atual é a de que a prevenção criminal deve ser coproduzida pelos diversos atores da sociedade e não apenas pelas forças de segurança (Elias, 2018). O propósito é atuar com vista a evitar o facto danoso, sendo para isso necessário entender-se as consequências e principalmente as causas da criminalidade (Elias, 2018). Nesta conformidade, há que atuar essencialmente ao nível da prevenção primária e secundária, isto é, nas causas e nos alvos. Mormente junto da população mais vulnerável, os jovens e os idosos.

Guedes et al. (2021) identificaram diversos estudos que revelam a propensão dos jovens à vitimação por cibercrime, devido à utilização elevada que fazem da *internet*. Um estudo realizado em 2020 pelo, ISPA e ISCTE, concluiu que 61,4% dos estudantes (ensino básico, secundário e superior) foram vítimas de *cyberbullying* em Portugal, durante o segundo confinamento (março a maio) (Lusa, 2020a). Em relação aos idosos, existe

semelhante tendência, devido "ao aumento de cibernautas idosos que apresentam um défice de literacia digital" (Poiares, 2019, p.119).

Khadas (2020) elenca quatro causas do cibercrime: a capacidade de um simples computador armazenar grandes quantidades de dados, o que facilita a aquisição dos mesmos pelos ofensores; a negligência que as pessoas cometem ao proteger o computador permitindo que o criminoso se aproveite dessas vulnerabilidades; o fácil acesso à informação das pessoas e consequentemente a sua utilização indevida e a perda de provas, na medida em que o infrator consegue apagar o seu rasto. Como argumenta Robalo (2021, p.51): "para cada cibercrime há uma causa", pois depende de que forma o ofensor se aproveitou da vulnerabilidade encontrada e qual era a sua intenção.

As estratégias de prevenção da criminalidade são divididas em primárias, secundárias e terciárias, identificando-se diferentes propósitos, atores e medidas. Brantingham e Faust (1976) apresentaram esta tripartição. A prevenção primária visa identificar as condições do ambiente social e físico que proporcionam facilidades e oportunidades para o cometimento de crimes, com o objetivo de as alterar, diminuindo o seu potencial criminógeno (Brantingham & Faust, 1976, p. 290). Englobam-se aqui ações como o *design* ambiental e a educação e sensibilização sobre o crime e a sua prevenção ao público em geral (Fisher & Lab, 2010; Elias, 2018). A prevenção secundária identifica situações, locais e grupos de risco, para minimizar a ocorrência de crimes e impedir que crianças e jovens enveredem por esse caminho (Fisher & Lab, 2010; Elias, 2018). Neste tipo de prevenção enquadra-se a prevenção situacional e o policiamento de proximidade. Por fim, na prevenção terciária, o intuito é reintegrar e reabilitar os ofensores para que não voltem a delinquir, pelo que o ator principal aqui é o sistema judiciário (Fisher & Lab, 2010; Elias, 2018).

Em suma, o propósito da prevenção da criminalidade é a redução da vitimação, sendo para isso, necessário, examinar primeiro as causas que potencialmente geram o ilícito e em segundo lugar, assegurar que a vítima e inclusive a comunidade ajam no sentido de diminuir as probabilidades de ocorrência de um crime, adotando medidas e estratégias preventivas (Costa, 2007).

1.5. Modelos de policiamento

1.5.1. Policiamento de proximidade

O policiamento de proximidade visa a aproximação da polícia à população, o que implica um maior conhecimento das suas rotinas e dos seus problemas (Lisboa & Teixeira, 2015). Os objetivos são a redução da criminalidade, o aumento do sentimento de segurança

e uma maior satisfação com o serviço policial (Rosenbaum & Lurigio, 1994). Desta forma, deve existir um trabalho conjunto entre os polícias e os cidadãos no sentido de encontrarem formas de solucionar os problemas que os afetam (Baker, 2006).

José de Oliveira (2002) caracteriza a proximidade com base em três dimensões: espacial, temporal e relacional. O primeiro elemento assume uma importância acrescida no contexto em estudo pois o ciberespaço é um ambiente em constante exploração e muito diferente do físico. O autor refere a aproximação física da Polícia à população, a perceção das especificidades do local e, por conseguinte, a adaptação das táticas. O elemento temporal diz respeito aos aspetos organizacionais e aos horários de trabalho e o fator relacional à qualidade do serviço policial, devendo-se pugnar pelo humanismo na resolução dos problemas e pela coesão social (Oliveira, 2002).

O modelo de policiamento de proximidade, implementado pela Polícia de Segurança Pública, integra-se no pilar da prevenção, articula-se com outras valências da PSP, como as informações e a investigação criminal, essenciais neste âmbito e é um policiamento que busca coproduzir a segurança com outros atores, não relegando esta tarefa apenas à PSP (Monjardet, 1996 as cited in Elias, 2009). Assim, procura identificar os problemas que mais afetam o sentimento de insegurança da população para os tentar resolver. Trata-se de uma abordagem proativa e simultaneamente preventiva do crime, em que são privilegiadas parcerias e focalizada a atenção nos grupos de risco (Diretiva Estratégica N.º10/2006). Nessa senda, surgem os programas especiais, direcionados a públicos-alvo específicos, como a *Escola Segura*, o *Comércio Seguro*, *Idosos em Segurança*, o *Significativo Azul* ou a *Internet mais Segur*a.

1.6. Modelo integrado de policiamento de proximidade na PSP

A Lei n.º 55/2020 de 23 de maio que define os objetivos, prioridades e orientações de política criminal para o biénio de 2020-2022, identifica a necessidade de serem desenvolvidos programas e planos de policiamento de proximidade, "destinados a proteger as vítimas especialmente vulneráveis, em especial as vítimas de violência em contexto familiar" fazendo menção ainda ao controlo dos "meios especialmente complexos, como a informática e a *Internet*" (art.º 9.º, n.º1). O terrorismo, os crimes de ódio, a extorsão, a burla informática, os crimes contra a liberdade e a autodeterminação sexual são alguns dos fenómenos cibernéticos elencados no anexo daquele preceito legal, para os quais existe a necessidade de assegurar esforços para a sua prevenção e repressão.

1.6.1. Diretiva estratégica n.º 10/2006 de 15 de maio

A Direção Nacional da PSP emitiu a Diretiva Estratégica 10/2006 relativa ao Programa Integrado de Policiamento de Proximidade e sua implementação, com o propósito de "melhorar a qualidade do serviço prestado ao cidadão, a melhoria dos índices de eficiência e de eficácia da atuação policial e de forma a efetivar-se uma maior articulação entre as valências de prevenção da criminalidade/proximidade, de ordem pública, de investigação criminal e de informações" (Diretiva Estratégica n.º10/2006 DN/PSP, p. 4). A grande diferença para o policiamento tradicional consiste na abordagem orientada para a resolução de problemas concretos que afetem o bem-estar e a segurança dos cidadãos. Isto é, os polícias continuam a desempenhar as tarefas ditas tradicionais, mas complementam-nas com uma estratégia de proximidade, em que existe a preocupação de solucionar os problemas/incivilidades antes que deem origem a formas criminais. Nesse sentido, são adotadas determinadas táticas de prevenção e combate ao crime por forma à obtenção de resultados que se prolonguem no tempo (Diretiva Estratégica n.º10/2006 DN/PSP). O policiamento repressivo tende a alcançar resultados a curto prazo, ao contrário do policiamento preventivo que só os vê a longo prazo, porém duradouros.

De acordo com a Diretiva Estratégica nº10/2006, o Comandante de Divisão ou de Esquadra é o gestor local do Policiamento de Proximidade, implementando-o na respetiva subunidade policial e efetuando o contacto com as entidades públicas (Câmara Municipal, Junta de Freguesia, etc.) e privadas. Existe também o supervisor local que é um chefe, responsável pelo acompanhamento, orientação e supervisão das Equipas de Proximidade e de Apoio à Vítima (EPAV) e das Equipas do Programa Escola Segura (EPES) que, também realiza contactos no âmbito de parcerias desenvolvidas com a PSP.

O MIIP é constituído pelas EPES e EPAV. Os agentes de proximidade afetos às primeiras são responsáveis pela segurança e vigilância nas áreas escolares, prevenção da delinquência juvenil, deteção de problemas que possam interferir na situação de segurança dos cidadãos e pela deteção de cifras negras no seio das comunidades escolares (Diretiva Estratégica n.º10/2006 DN/PSP). As segundas equipas têm a seu cargo a vigilância das áreas comerciais, das áreas residenciais preferencialmente as habitadas por cidadãos idosos, a prevenção da violência doméstica, o apoio e acompanhamento das vítimas de crime e ainda a identificação de problemas que aumentem o sentimento de insegurança da população e, consequentemente as cifras negras. São formadas equipas de proximidade afetas a um determinado setor da área de responsabilidade da esquadra, devendo-se manter fixas por um

período de tempo razoável para um melhor conhecimento dos problemas dos cidadãos residentes e das inurbanidades e ilícitos criminais da zona e maior aproximação e contacto com a população e entidades competentes (Diretiva Estratégica n.º10/2006 DN/PSP). Outra especificidade importante deste Programa é a responsabilização conferida àqueles agentes, que têm como funções, entre outras: garantir a segurança e visibilidade na via pública e nas áreas escolares; prevenir a ocorrência de delitos criminais nas áreas residenciais e comerciais; estabelecer contactos periódicos com os comerciantes, residentes e visitantes habituais no setor onde prestam serviço; realizar ações de sensibilização ou propor ao escalão superior; efetuar o diagnóstico da situação de segurança no seu setor; assegurar o atendimento e apoio às vítimas de crime; procurar a colaboração do público e fornecer-lhe informações úteis; identificar problemas e ainda recolher informações acerca de ilícitos criminais e dos seus suspeitos e sobre possíveis locais de vigilância (Diretiva Estratégica n.º10/2006 DN/PSP). De acordo com Elias (2007, p. 482), estes agentes possuem um papel fundamental na obtenção de informações porque conhecem as fragilidades e potencialidades do meio e ainda pelo contacto próximo que estabelecem com o público-alvo mais vulnerável (crianças, jovens, idosos, habitantes de zonas urbanas sensíveis, etc.), sendo utilizadas posteriormente pelos elementos da investigação criminal, das informações criminais e até como apoio à decisão do comandante de esquadra.

O policiamento de proximidade, tal como está expresso na Diretiva Estratégica n.º10/2006 DN/PSP, é mais eficaz porque "mobiliza a comunidade na prevenção e combate ao crime; utiliza conjuntamente os recursos comunitários e policiais no combate ao crime; previne e combate as causas do crime e incivilidades em parceria com a comunidade; está mais próximo dos problemas, tendo mais possibilidades de os identificar e resolver e utiliza a comunidade como fonte de informação e apoio" (pp. 5-6). O MIPP é "patrulhar sem pressa"; de forma direcionada; é prevenção; é verem e serem vistos; é parceria porque a segurança começa em cada um de nós, com o propósito de conhecer as pessoas e cuidá-las continuamente.

1.6.2. Adaptação do MIPP ao ciberespaço

O ciberespaço é caracterizado, por Mendonça (2021), como sendo aterritorial, isto é, não possui barreiras físicas ou delimitações; onde impera uma gestão descentralizada pois não existe uma única pessoa que o comande; confere um elevado grau de anonimização; considerado um espaço não mediado; um "megafone planetário" (Martins & Garcia, 2013, as cited in Mendonça, 2021); um catalisador para a ação coletiva (Santos & Guedes, 2015)

e possibilita igualmente uma simultaneidade de efeitos a uma velocidade sem precedentes. Neste sentido, cria constantemente novos desafios, o que exige métodos e meios de intervenção especializados e sofisticados que os consigam acompanhar.

Adaptar o MIPP ao ciberespaço não consubstancia tarefa fácil pois está direcionado para as pessoas e o seu meio envolvente (família, habitação, bairro, pares, escola, etc.), meio esse que é físico, concreto e não virtual, como é o caso da *internet*. No entanto, a rede tecnológica em que vivemos é feita de e por pessoas, pelo que estas devem ser o princípio base para a implementação de um Programa de Policiamento de Proximidade. As maiores ameaças que surgem neste contexto são a apatia, a ignorância ou não consciência e a iliteracia digital (Mendonça, 2021). Assim, a componente humana deve integrar toda a estratégia de cibersegurança.

Com base na Diretiva Estratégica n.º10/2006, no estado de arte e nas informações recolhidas através das entrevistas e adaptando a realidade atual ao ciberespaço, é possível tecer algumas considerações. Primeiramente é necessário efetuar-se uma análise estatística relativa à criminalidade denunciada, se possível aplicar inquéritos junto da população, com o intuito de conhecer a criminalidade denunciada, o sentimento subjetivo de insegurança e o medo dos cidadãos (Elias, 2007), daí que um dos objetivos do presente estudo se insira nesse ponto. Deve ser realizada uma caracterização quer das vítimas, quer dos ofensores, do espaço e das tipologias criminais, tentando-se correlacionar algumas ideias, como se procedeu no capítulo 1.3. Este diagnóstico permite focalizar as ações de prevenção e de repressão ao cibercrime.

Em segundo lugar, têm de ser estabelecidos objetivos concretos e mensuráveis para o trabalho do MIPP no ciberespaço: o ponto de partida tem de ser a consciencialização; a necessidade de programas de capacitação de cidadãos em cibersegurança; a cooperação/parceria com outras entidades, nomeadamente o CNCS e o acompanhamento pós-vitimação. Desta forma, podem-se enquadrar no ciberespaço os seguintes objetivos operacionais presentes na Diretiva Estratégica n.º10/2006: reduzir os índices de insegurança objetiva e subjetiva; reduzir a criminalidade; focalizar a atenção da Polícia nos grupos de risco; aumentar os índices de participação de crimes à Polícia e dar conteúdo preventivo aos cidadãos. A cibersegurança é um tema afeto a todas as pessoas, não obstante a predominância dever ser o público mais vulnerável, as crianças e jovens e os idosos. Esta área integra-se noutros programas, como no *Comércio Seguro*, porquanto a burla informática é dos fenómenos criminais mais recorrentes, no *Idosos em Segurança*, pois apresentam uma taxa de iliteracia tecnológica muito elevada e na *Escola Segura* e *Universidade Segura*, no

sentido em que estas temáticas devem ser abordadas nos ensinos básico, secundário e superior.

No que aos agentes de proximidade diz respeito, estes devem ter formação na área da cibersegurança, da vitimologia e da psicologia, possuir um bom relacionamento interpessoal, uma boa expressão oral e iniciativa para desenvolver ações (Elias, 2007). No caso em apreço, não existirão setores, pois trata-se de um espaço maioritariamente não físico. O objetivo aqui será a especialização do efetivo por áreas temáticas. Todo o tipo de informação que lhes chegar, útil para posterior investigação, deverá ser encaminhada para o dispositivo de informações policiais ou de investigação criminal (Elias, 2007), ou neste caso, primeiramente para o Núcleo de Cibercriminalidade.

Relativamente aos objetivos, em ordem a reduzir o sentimento de insegurança, os cidadãos têm de ser consciencializados para os riscos que os seus comportamentos podem causar. A cibersegurança não é apenas um problema técnico, criminal ou político, é um problema social, que enfrenta técnicas generalizadas de engenharia social, isto é, "o ato de enganar um indivíduo no sentido de este revelar informação sensível, obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança" (Grassi et al., 2017, p. 54). Desta forma, as pessoas têm de ser elucidadas acerca destes tipos de persuasão para não serem enganadas. Primordialmente especial importância com a capacitação de crianças, adolescentes, população sénior e outros grupos de risco.

Em relação às crianças e jovens tem de existir uma colaboração do MIPP com as escolas, em vista a reforçar as competências e conhecimentos em segurança do ciberespaço, inclusive incluir esta matéria nos planos curriculares. Além disso, deve ser proporcionada formação contínua aos professores e assistentes operacionais e muito importante, a identificação de jovens com alto potencial para esta área e a promoção da sua integração atempada em contexto profissional, como previsto na ENSC 2019-2023. Outra medida a implementar é a educação e sensibilização dos pais destas crianças e adolescentes, porquanto têm de estar consciencializados do perigo de estar *online* e incutir boas práticas nos seus descendentes (controlo parental). Em março de 2021, o Comité para os Direitos das Crianças (CRC) adotou o *General Comment* n.º 25 sobre os Direitos da Criança em ambiente digital, um marco importante em que se preconiza que os seus direitos se aplicam tanto *offline* como *online* (Livingstone, 2021).

Contrariamente aos mais jovens, que passam largas horas *online*, a população sénior tem um contacto mínimo com as TIC, como evidenciam os estudos (Loos, 2011; Gil &

Amaro, 2011; Dias, 2012; Gil, 2016; Gil, 2019; Alcobia et al., 2020). A reduzida exposição às TIC durante grande parte da vida, as limitações ao nível das funções cognitivas e biológicas/físicas com o avançar da idade, a falta de experiência, a menor escolaridade e consequente dificuldade na aprendizagem digital (Gil & Amaro, 2011; Loos, 2011; Coelho, 2019; Alcobia et al., 2020), são fatores que levam à exclusão digital. Apesar de a percentagem de indivíduos dos 65-74 anos que utilizam a *internet* em Portugal ter vindo a aumentar, especialmente no ano de 2021 (47,7%) face a 2020 (39%) (PORDATA, 2021), ainda representam valores diminutos. Desta forma, é sentida a necessidade de desenvolver e apoiar práticas que os motivem e ajudem no uso do computador e *internet*. Os objetivos do MIPP deverão ter em conta três vetores: o desenvolvimento de competências digitais, nomeadamente através de ações de formação; a promoção da educação para a sensibilização da importância, utilidade e funcionalidade da tecnologia e ainda informar acerca dos riscos que podem correr (Alcobia et al., 2020). O propósito é a sua inclusão digital de uma forma consciente, informada e responsável.

No que se refere às ações de sensibilização/formação são analisadas as Diretivas Estratégicas N.º 43/2021 "*Bullying* é Para Fracos", N.º 55/2021 "A violência fica à porta", N.º3/2022 "*Internet* Mais Segura" e N.º5/2022 "No Namoro Não Há Guerra". Na segunda e quartas Diretivas mencionadas, não se encontra qualquer referência relativa à sua possível perpetuação pela *internet* ou através de meios digitais. Na primeira, que é a mais antiga, é notado o recurso às novas tecnologias "que promovem uma rápida expansão de imagens e mensagens promotoras de insegurança" e às redes sociais, "divergindo da vertente física da provocação, ameaça, intimidação e vitimação entre alunos, para a virtual, o *ciberbullying"* (ponto (6)). A DIREST da *Internet* Mais Segura expõe de igual forma o referido na primeira, reforçando os riscos e ameaças que a *internet* pode veicular e o aproveitamento face às vulnerabilidades dos mais jovens. Como resposta, são assinaladas a Diretiva Operacional n.º30/2014 "Um Conto pelas Crianças", a coleção "Eu Faço Como Diz o Falco" e o Programa "Comunicar em Segurança", com conteúdos formativos direcionados para cada ciclo do ensino básico e ensino secundário. Por exemplo, nas faixas etárias mais elevadas, são introduzidos temas como o *sexting*, os jogos e apostas, as compras e a dependência *online*.

Os agentes de proximidade têm ainda um papel ativo ao nível do acompanhamento pós-vitimação, pois pode ser uma experiência difícil para a vítima, tendo como consequências: o sentimento de culpa ou vergonha, injustiça, solidão, ansiedade e insegurança, medo, entre outros (APAVparajovens, s.d). Um exemplo concreto é o caso do

crime de burla, que, para além de causar prejuízo financeiro, a vítima pode experienciar sintomas como *flashbacks*, ansiedade, dificuldade em dormir, sentimento de culpa, raiva, medo, mudanças de humor, perturbações de ordem física (distúrbios na alimentação, dores no peito, tonturas, dores de cabeça e nas costas, etc.) e as reações das pessoas próximas da vítima podem ainda aumentar os sentimentos de culpa e de vergonha (APAV, 2020).

Capítulo 2: Vertentes de intervenção da PSP na prevenção de ilícitos no ciberespaço

Como notado anteriormente, a PSP contribui para a prevenção do cibercrime. Ao nível da prevenção primária, o foco é o controlo social externo (família, escola, comunidade, trabalho), quanto à secundária incide sobre os autores e a terciária diz respeito aos alvos (objetos, espaços e situações) (Santos et al., 2008). Os pilares da formação e sensibilização são os que prevalecem na missão do MIPP, contudo, a PSP também investiga e como não é um ator isolado, a coprodução da segurança é igualmente deveras significativa.

2.1. Formação

Em termos de formação, e integrando-se na prevenção secundária, a PSP carece de investimento na especialização dos seus elementos, apesar da criação de uma unidade especializada, o Núcleo de Cibercriminalidade no Departamento de Investigação Criminal da Direção Nacional da PSP, em novembro de 2020, tendo iniciado funções em janeiro de 2021. O objetivo da sua implementação é "apoiar a Estrutura de Investigação Criminal, nomeadamente, na prevenção, deteção e investigação de condutas ilícitas, cometidas com auxílio dos meios informáticos, no âmbito das competências da Polícia de Segurança Pública ", de acordo com o Despacho n.º 6158/2017, que o originou. Uma das preocupações iniciais aquando da implementação do Núcleo, foi, exatamente, a formação do efetivo. Esta Polícia deve possuir uma estrutura que permita a investigação dos crimes da sua competência mas praticados noutro espaço, "como uma extensão das suas atribuições no mundo não virtual" (Machado, 2015, p.41). Por outro lado, assim como os agentes do MIPP são formados para matérias como a violência doméstica ou a avaliação do potencial de mudança nas famílias, também devem sê-lo em relação à cibersegurança, cibereducação e ciberhigiene.

2.2. Sensibilização

Existem dois centros de sensibilização a nível nacional: um operacionalizado pelo CIS direcionado a toda a população, em que são promovidas campanhas informativas e de sensibilização e instrumentos e ferramentas para capacitar os cidadãos com as necessárias competências digitais e o SeguraNet, da responsabilidade da Direção-Geral da Educação

dirigido à comunidade escolar (CNCS, 2021c). A colaboração com estas entidades seria uma mais-valia para a PSP, uma vez que esta é quem está mais próxima da população em geral e dos alunos em particular, portanto tem um papel ativo na implementação de uma cultura de segurança, minimizando os riscos provenientes das plataformas digitais.

A ENSC 2019-2023 define 6 eixos de ação, entre os quais o segundo "Prevenção, educação e sensibilização" devido à importância de antecipar ameaças, de informar, sensibilizar e consciencializar. Salientam-se as seguintes medidas: estimular nos cidadãos o desenvolvimento de competências digitais, educar para uma utilização segura, consciente e responsável das tecnologias digitais e promover programas de capacitação em cibersegurança quer para as organizações, quer para o cidadão comum, com especial enfoque nas crianças, adolescentes, população sénior e outros grupos de risco (CNCS, 2019).

Esta vertente de atuação é fundamental no trabalho do MIPP, pois é o primeiro passo para a prevenção da cibercriminalidade, uma vez que os utilizadores são a componente que realmente importa, sendo responsáveis por muitos ataques de cibersegurança e por falhas de segurança. A prioridade devem ser os grupos etários e sociais mais vulneráveis. A primeira referência ao MIPP encontrada, no que concerne aos crimes na *internet*, vem na Revista Polícia Portuguesa de 2012 "Manifestações", uma conferência realizada em Castelo Branco, para 600 alunos, em parceira com a PJ e a Universidade da Beira Interior (N. B. M, 2012, p. 22). Em 2020, o Programa Escola Segura sobre a utilização segura da *internet* realizou 1465 ações, com a sensibilização de 30.395 alunos, enquanto o Programa Apoio 65 – Idosos em Segurança sobre a utilização segura da *internet*, efetuou 22 ações, com a sensibilização de 404 idosos. Em 2021, estes números sofreram uma grande descida, com 618 ações e 10778 alunos sensibilizados, no primeiro programa e 7 ações e 51 idosos sensibilizados, no segundo programa[1].

2.2.1. Idosos

A literacia digital define-se, pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (2018, p. 6), como "a capacidade de aceder, gerir, compreender, integrar, comunicar, avaliar e criar informação de forma segura e adequada através das tecnologias digitais". A literacia digital é uma preocupação atual vista como uma competência essencial à aprendizagem ao longo da vida (Costa et al.,2015). Em relação aos

[1] Segundo informação fornecida pela Direção Nacional da Polícia de Segurança Pública, cuja autorização encontra-se no Apêndice A.

mais seniores, note-se alguns fatores de bem-estar fornecidos pelas tecnologias digitais: a necessidade de atualizar conhecimentos; estar ativo intelectualmente; utilizar melhor o computador (Gil & Páscoa, 2018); o fomento de relações sociais; auxílio em áreas como a saúde, o acesso a serviços, etc.; o desfrutar do tempo de forma diferente (Dias, 2012); as redes sociais podem ser um aliado na superação da sensação de solidão, na redução da ansiedade e na promoção de perceções de controlo e autoeficácia (Leist, 2013). Não obstante estas vantagens, referir que estas apenas se podem manifestar caso haja uma correta e segura utilização das plataformas *online*.

Os idosos são um alvo apetecível para os cibercriminosos devido, por via de regra, à ausência de competências digitais e à sua vulnerabilidade e inocência. Através de ataques de engenharia social torna-se fácil obter certo tipo de informação ou levar alguém a praticar certa conduta, especialmente tratando-se de pessoas mais velhas, sem conhecimentos e vivendo sozinhas. Uma preocupação que está a crescer no seio deste público-alvo são as "ciberburlas românticas", que, para além de gerarem perdas monetárias, geram um sentimento de vergonha e culpa nas vítimas, inibindo-as de apresentar queixa às autoridades (Guimarães, 2018). Sendo difícil para uma pessoa letrada digitalmente identificar um ataque, dado o grau de sofisticação, acresce a dificuldade ainda mais para estes. Assim, os agentes de proximidade são responsáveis pela educação e sensibilização destas pessoas, seja através de ações de formação, de sensibilização (ex. o projeto literacia digital de adultos "Lidia"), aulas, auxílio em casa, distribuição de panfletos e de guias de boas práticas ou até da criação de uma linha telefónica específica para ajudar a detetar fraudes, burlas, etc., entre outras medidas.

2.2.2. Crianças e jovens

O uso das tecnologias digitais é cada vez mais precoce (Dias & Brito, 2021, p.7). Uma em cada três crianças utiliza a *internet* (UNICEF, 2019), sendo as idades dos 15 aos 24 anos, o escalão etário que mais se conecta *online* (UNICEF, 2017). O *Estudo EU Kids Online 2020* aferiu que o tempo que as crianças e jovens, em Portugal, passam *online* mais do que duplicou face ao estudo de 2010 (Smahel, 2020). As crianças, atualmente, são chamadas de "nativos digitais" (Lança, 2014, p.93), no entanto, não se nasce digital (Ponte, 2020). As crianças não conseguem perceber de que se trata a *internet* ou quais os riscos e vantagens a ela associadas (Patrão et al., 2021). Sabendo que a sua utilização é praticamente inevitável, há que procurar identificar formas de assegurar que esta é feita de forma segura, consciente,

crítica e benéfica (Dias & Brito, 2021). A investigação científica é igualmente crucial para conhecermos como as crianças e jovens estão a usar a *internet*, o que significa para elas, quais os riscos e/ou oportunidades, a sua vitimação e ainda a relação entre elas e o mundo mediado pelas tecnologias, ou seja, os contextos em que estão inseridos: a cultura de pares, a socialização familiar, o ambiente escolar e da comunidade onde vivem, a ecologia do digital (Ponte, 2020). Daí um dos objetivos desta dissertação e a consequente aplicação de um inquérito adaptado do *EU Kids Online*, tendo em consideração as crianças mais jovens, que, devido a alguns constrangimentos, não têm sido incorporadas nos estudos, como assinalado por Dias e Brito (2021).

Ramalho (2021), no seu estudo acerca dos efeitos que a utilização da tecnologia terá no desenvolvimento das crianças mais jovens, identifica algumas potencialidades: "o jogo *online* parece estimular o desenvolvimento cognitivo (reconhecimento de padrões e memória visual) " (p.21); "a aquisição de aptidões operacionais" (p.23); o "aprofundamento de conhecimentos e da sua compreensão acerca do mundo" (p.23); o "desenvolvimento de disposições para a aprendizagem no domínio cognitivo e sócio-emocional" (p.23); "compreensão do papel da tecnologia na vida quotidiana" (p.23); estimula o pensamento criativo (p.24). Por outro lado, a autora refere alguns riscos como, o facto de o jogo *online* se poder relacionar também com a distratibilidade, sobreativação, hostilidade e agressão; a imitação e a demonstração por parte dos pais e irmãos mais velhos, levando a criança a adotar o mesmo comportamento; uso excessivo em detrimento de outras atividades; afetação do desenvolvimento social, cognitivo e linguístico; contactos perigosos ou comportamentos impróprios; aspetos ligados à saúde. Aponta também que as crianças mais vulneráveis são as do sexo feminino, as que vivem em ambientes familiares socialmente desfavorecidos, as que apresentam deficiência ou algum desajustamento psicológico, as crianças de grupos marginalizados e as cujo acesso ao mundo digital não é guiado (Ramalho, 2021).

Lança (2014) sustenta que a maior vulnerabilidade dos jovens é o excesso de confiança, sentindo-se seguros a navegar pela *internet*, assumindo comportamentos de risco, residindo aí a preocupação: nas ameaças a que ficam sujeitos. O autor destaca a pornografia, a pedofilia, o assédio sexual, práticas comerciais abusivas, *cyberbullying* e/ou *stalking*, fóruns pró-suicídio, pró-autoflagelação, pró-anorexias e pró-bulimia, o discurso de ódio, a exposição à violência e a pirataria e adição aos jogos, como as principais ameaças.

Para minimizar estes riscos é preciso promover junto das crianças atividades que fomentem a literacia digital e bons hábitos *online*, educar e sensibilizar para as potencialidades mas também para os perigos, ajudar a que desenvolvam capacidades sociais

e construam relações físicas, é importante a mediação parental e o estabelecimento de regras em casa (APA, 2019) e ainda a identificação de possíveis indícios de estarem a ser alvo de um predador *online*, como indicam Santos e Manteigas (2010, pp.86 e 87). "Se formos capazes de proteger as crianças do pior que as tecnologias digitais podem fazer acontecer, ampliamos o seu acesso ao melhor e às mais ricas possibilidades que elas têm para oferecer" (Ramalho, 2021, p.16), é esta a ideia que deve sempre prevalecer e não privá-las totalmente do seu uso.

2.3. Colaboração nacional sobre cibersegurança e cibercrime

Para além da colaboração com outras Forças de Segurança nacionais, nomeadamente a Guarda Nacional Republicana e a PJ, em termos de investigação da cibercriminalidade, poderá existir uma relação institucional entre a PSP e o Centro Nacional de Cibersegurança e a Direção-Geral da Educação, como constatado anteriormente, nos planos da sensibilização e educação. Segundo o Observatório de Cibersegurança, no *Relatório Cibersegurança em Portugal: Sociedade 2021*, em 2020, houve um aumento do volume de uso do correio eletrónico, videochamadas, mensagens instantâneas, pesquisas de informação *online*, banca *online* e comércio eletrónico e do trabalho remoto (CNCS, 2021d). A utilização das redes sociais em Portugal é muito superior à média da UE, sendo que são plataformas que potenciam a ocorrência de práticas ligadas à engenharia social, como a desinformação, o roubo de identidade, o *phishing*, a burla/fraude e a criação de perfis de utilizadores para fins maliciosos (CNCS, 2021d). A desinformação pode afetar a forma como os indivíduos percecionam o mundo e consequentemente o ambiente do ciberespaço, o que poderá ter implicações ao nível da qualidade da democracia e na cibersegurança (CNCS, 2021d). Neste sentido, surgem as parcerias, que têm um impacto tremendo na prevenção e na recolha e troca de informação se forem ativas e contínuas envolvendo as escolas, universidades, por exemplo, o Laboratório de cibercrime do Instituto Politécnico de Beja, que colabora com a PJ e organiza Simpósios de Segurança Informática e de Cibercrime, comunidades, empresas de segurança, empresas em geral, comerciantes, bancos, redes de comunicações (MEO, Vodafone, OLX, Microsoft, *facebook*, *twitter*), marcas do ramo automóvel, órgãos de comunicação social regionais/locais/nacionais, entre outros.

2.4. Cooperação internacional

A complexidade dos crimes, e a ausência de fronteiras no domínio do ciberespaço, faz com que estes sejam transnacionais, isto é, o (s) local (ais) onde foi perpetrado é diferente do sítio (s) onde se deram as consequências de tal facto criminoso, o que dificulta a

investigação e a descoberta do autor material do ilícito. Além disso, os números de cibercrimes assim como os utilizadores das tecnologias digitais não param de aumentar, evidenciando que, apesar dos esforços em sensibilizar e educar os cidadãos, têm-se revelado insuficientes ou pouco eficazes. Dessarte, é essencial ter em consideração e estar a par das práticas e medidas que outros países implementam nesta matéria, analisar a sua eficácia e equacionar a sua concretização em Portugal. Igualmente relevante são os vários atores que se encarregam da cibersegurança dos Estados, do setor privado e dos cidadãos, como a European Union Agency for Cybersecurity (ENISA), a EUROPOL/EC3 e a European Malware Anaylsis Solution (EMAS), a Agência Europeia de Defesa (AED), também a ONU, a INTERPOL e o Conselho da Europa, que emanam regulamentos, relatórios, resoluções, convenções, diretivas (Elias, 2018) - importantes instrumentos de apoio à prevenção e ao combate do cibercrime. De ressalvar a criação recente de um Projeto inovador da EUROPOL, do qual a PSP faz parte, "EMPACT", que conta com a participação de vários países e agências e que se baseia na dissuasão de potenciais cibercriminosos enveredarem por caminhos ilícitos, consciencializando sobre a ilicitude e consequências dos atos e informando sobre caminhos alternativos, segundo informação fornecida pela Chefe do NCiber, a título informal.

Em 2013 criou-se a unidade EC3 (*European CyberCrime Centre)* no seio da Europol, com a finalidade de conferir apoio e coordenar investigações levadas a cabo pelos Estados-membro, sobre crimes informáticos, porém, como argumenta Armando Dias Ramos (2022), trata-se tão-só de um canal de informação célere entre os vários países da UE que, porventura, no caso de um Estado Membro não fornecer a informação solicitada por um órgão policial, no âmbito de um processo-crime, esta unidade não tem competência para intervir. Não obstante, a EC3 é um ponto de partilha de informação precioso, compilando os *modus operandi* recentes e é responsável por coordenar as operações de combate ao cibercrime a nível europeu (Ramos, 2022). Por seu turno, é a Europol que faz a ligação entre o país que, no decurso de uma investigação deteta um IP de outro país e este de onde provém o IP para a prossecução da investigação neste último (Ramos, 2022).

De realçar que a Diretiva 2006/24/CE (Lei n.º 32/2008 de 17 de julho no contexto nacional), referente à conservação de dados gerados ou tratados no contexto da oferta de serviços de comunicações eletrónicas publicamente disponíveis ou de redes públicas de comunicações, já foi considerada inválida pela Grande Secção do Tribunal de Justiça, em 2014, resultando na abstenção, por parte de alguns países da EU, de legislar sobre a retenção de dados e consequentemente na ausência de resposta a pedidos de fornecimento de

informação quando os IP´s são identificados no seu território (Ramos, 2022). Ora este facto prejudica ainda mais a obtenção da identidade dos autores dos crimes e a eficácia da IC e da justiça, em especial em Portugal, onde aquela Lei continua em vigor.

Em Espanha, quando os criminosos recorrem a redes disponíveis e acessíveis a todos para perpetrar ataques, é obrigatório que quem disponibiliza esse ponto de acesso à *internet* faculte os dados dos utilizadores que estiveram ligados, para a sua identificação, pois se não o fizer, incorre numa contraordenação, cuja coima vai de trinta mil euros a cento e cinquenta mil euros (*Ley general de telecomunicaciones,* Lei n.º 9/2014, de 9 de maio, art.º 79.º). Já em Portugal, tal não acontece, pois não existe norma legal que responsabilize quem fornece *wi-fi*, *acess point* ou *wireless* (Ramos, 2022).

2.5. Investigação criminal

A PSP encontra-se nos primórdios da investigação do crime *online*, existindo pouca formação e escassos recursos materiais e humanos, segundo a posição do chefe do Núcleo de Apoio Operacional e da chefe do NCiber.[2] Começou-se a desenvolver mais trabalho nesta área a partir da criação do Núcleo de Cibercriminalidade, onde se dá apoio à estrutura de IC no âmbito da prevenção, deteção e investigação de cibercrimes da competência da PSP (cfr. Despacho n.º 6158/2017), se forma o efetivo nestas matérias (têm formação contínua), se faz a monitorização de fontes abertas e se emitem Alertas Operacionais. Em 2021, o Nciber apoiou 53 inquéritos criminais, alguns como um pedido de apoio ou pedido adicional de informação quando surgem novos dados e apoiou 54 pedidos de recolha de informação (identificação de suspeitos nas redes sociais, identificação de IP´s (*Internet Protocol)*, seus utilizadores e mensagens de correio eletrónico).

No que refere à monitorização de fontes abertas, o trabalho do NCiber consiste em obter informação permanente e atual acerca de suspeitos já identificados ou identificar possíveis criminosos, maioritariamente nas redes sociais, assim como em fóruns de conversação por forma a conhecer os seus frequentadores e o tipo de informação que ali circula, com vista a identificar fenómenos ou ilícitos criminais ou ainda na *dark web*.[3] De notar que a criação de um perfil falso nas redes sociais demora tempo para que seja credível. O FBI, por exemplo, compra perfis já criados, com publicações e amigos para levar os

[2] Conforme entrevista dada no dia 10FEV2022 e 11FEV2022, pela Chefe do Núcleo de Cibercriminalidade e pelo Chefe do Núcleo de Apoio Operacional. Para mais detalhes, consultar APÊNDICE G.
[3] Conforme entrevista dada no dia 10FEV2022, pela Chefe do Núcleo de Cibercriminalidade. Para mais detalhes, consultar APÊNDICE G.

suspeitos a aceitarem o pedido de amizade (Ramos, 2022). Um caso conhecido e que levantou dúvidas em termos legais, sendo este método de recolha de prova proibido na maior parte dos países, foi a criação de uma boneca virtual, com a aparência de uma menina filipina pela ONG *Terre des Hommes*, com o objetivo de identificar predadores sexuais (Ramos, 2022). Os alertas operacionais, acerca de tipologias criminais a decorrer, a nível nacional, são direcionados quer para o público interno, os polícias, quer para o externo, a população em geral e órgãos de comunicação social.

Armando Dias Ramos (2022) defende que a recolha de informação em OSINT (*Open Source Intelligence*) possui algumas vantagens, tais como: a facilidade de obtenção e salvaguarda; a disponibilização da informação a qualquer momento; não necessitar de permissões legais das autoridades judiciárias; ser obtida em tempo real (principalmente nas redes sociais) e a possibilidade de corroboração com outras fontes de informação. Não obstante, podemos estar perante informação falsa, pelo que é necessário um processo mais complexo para validar os dados obtidos e, pelo facto de estar disponível ao público, qualquer um consegue fazer este trabalho (Ramos, 2022). Assim, à semelhança dos cibercriminosos, as autoridades de IC podem valer-se de práticas de engenharia social para a obtenção de informação valiosa sobre fenómenos e indivíduos, que, ao conseguir decifrar o seu perfil psicológico, torna-se possível identificar autores de ilícitos criminais (Mendes, 2014; Bravo, 2014; Ramos, 2022).

Apesar de ser importante este trabalho investigatório, urge recordar a dificuldade em identificar os cibercriminosos. A vertente da repressão complementa a vertente preventiva.

Capítulo 3: Vitimação (cibernética) das crianças e jovens

A vitimologia é um domínio científico cujo objeto de estudo são as vítimas de crimes e os objetivos passam por compreender as causas da vitimação, as suas consequências, a relação vítima-agressor, como o sistema criminal e de justiça atua e trata as vítimas e ainda de que forma estas são expostas por outros setores da sociedade, por exemplo, os *media* (Daigle, 2018; Halder, 2022). Nesta subárea da criminologia, procura-se responder à pergunta: "porque razão aquela pessoa foi vítima de determinado crime?"; assim, foram sendo disseminadas possíveis explicações ao longo dos anos nesse sentido, como: a teoria do estilo de vida, a teoria das atividades de rotina ou a teoria das janelas partidas (Robalo, 2021); a divisão das vítimas em categorias por Benjamin Mendelsohn; a enfatização da culpabilização da vítima; a importância conferida aos traços físicos, sexo, idade, aspetos

psicológicos, estatuto geo-político-social, etc. por Hans Von Hentig, entre outras (Halder, 2022). Clevenger et al. (2018) defendem a existência de características que tornam alguns indivíduos alvos atrativos, *verbi gratia* a vulnerabilidade e a incapacidade de compreender ou de relatar, necessitando de recursos adicionais e uma maior consideração. Os autores identificam nessa condição: as pessoas que se encontram presas, as pessoas com deficiências, as pessoas mais velhas, as pessoas com doenças mentais e os menores (Clevenger et al., 2018).

A cibervitimologia pode ser definida como "*the study of the causation of victimisation, patterns of victimisation and victimhood, the impact of victimisation, and the treatment of victims of cyber-crimes*" (Halder, 2022, p.7). Na presente investigação, o foco são as crianças e jovens que, juntamente com as mulheres, representam os grupos mais vulneráveis no ciberespaço (Halder, 2022). Por sua vez, segundo a UNICEF (2017), existem crianças mais vulneráveis aos perigos *online* do que outras, sendo estas as do sexo feminino, as de famílias pobres, as de comunidades retrógradas em relação às diferentes formas de abuso e exploração sexual de crianças, as que não vão à escola, as que possuem deficiências, as que sofrem de depressão ou de outros problemas de saúde mental e as que são marginalizadas no seu seio familiar.

3.1. *Cyberbullying*

Como anteriormente constatado, o surgimento da *internet* e dos meios tecnológicos potenciou tanto novas formas de cometer os tradicionais crimes como o aparecimento de um conjunto de novos crimes. O *bullying* já existia muito antes das tecnologias digitais, porém o ciberespaço confere determinadas características distintas do meio físico que facilitam a ação dos cibercriminosos e por conseguinte o *cyberbullying*, embora as definições andem par a par. Segundo Weber e Pelfrey (2014, pp. 33-34), *cyberbullying* é um "ato agressivo intencional realizado por um indivíduo ou por um grupo, utilizando formas de contacto por meio de telemóveis, computadores e dispositivos portáteis, repetidamente e perpetuado no tempo, contra uma vítima que não se pode defender facilmente". Concretamente, ocorre quando uma criança ou um adolescente, aproveitando-se do anonimato conferido pela *internet*, intimida, provoca, discrimina, ameaça, atormenta, importuna ou amedronta outrem (Santos & Manteigas, 2010). Este tipo de comportamento pode escalar até às ameaças de ofensas corporais e de vida (Santos & Manteigas, 2010), extrapolando-se para o mundo *offline*.

Os elementos mais associados a este fenómeno criminal e igualmente presentes no *bullying* tradicional são: a intenção, a repetição (contudo uma ação isolada pode ser disseminada para milhares de pessoas) e o desequilíbrio de poder entre a vítima e o ofensor, associado a diferentes capacidades tecnológicas, ao anonimato e ao medo provocado no alvo (Dooley et al., 2009; Betts, 2016). Além disso, existem outros aspetos que o diferenciam, como: ser uma forma de agressão indireta, o que favorece a condição de invisibilidade e de anonimato do *cyberbully* (Smith, 2013); nesse sentido, o não visionamento da reação da vítima nem o seu sofrimento, permite um distanciamento moral do *cyberbully* para com ela, o que facilita o *cyberbullying* na medida em que a empatia e o arrependimento são pouco prováveis (Smith, 2013; Navarro et al., 2016); o perpetrador pode ser desconhecido do alvo e os atos podem ser vistos por uma audiência ilimitada (Betts, 2016) e por um período temporal incógnito (Marczak & Coyne, 2015); o agressor tem acesso às vítimas 24H/7, pelo que, ao contrário do *bullying* tradicional, aquelas não têm onde se esconder (Smith, 2013), sendo a fronteira do ambiente escolar ultrapassada (Santos et al., 2021). Além disso, o tipo de emoção que provoca é também distinto do causado cara-a-cara (Englander, 2020).

Os telemóveis (chamadas, mensagens de texto), a *internet* (e.g., *e-mail*, plataformas de conversa *online*, *sites*) e as redes sociais são os meios mais comuns para cometer este tipo de ato (Santos et al., 2021), podendo assumir diferentes formas, desde difamação a *cyberstalking* ou assédio. Durante a juventude, 20 a 40% das crianças e adolescentes vão encontrar ou já encontraram alguma forma de *cyberbullying*, sendo que a idade em que são mais suscetíveis à vitimação é entre os 12 e os 14 anos (Tokunaga, 2010).

No que tange aos fatores de risco para a perpetração destes comportamentos, verifica-se, com base em revisões feitas por Tokunaga (2010), Chen, Ho e Lwin (2017) e Kowalski, Limber e McCord (2018) o seguinte: a utilização frequente de meios tecnológicos, o envolvimento em situações de *bullying* tradicional, o facto de ser mulher, ser LGBTQIA^{+}, níveis baixos de autoestima, autocontrolo e empatia, níveis altos de ansiedade, impulsividade, agressividade e desvinculação moral, depressão, o mau aproveitamento escolar e o mau ambiente familiar e escolar constituem os maiores preditores desta conduta; em oposição, elevados níveis de competências sociais, empatia, controlo das emoções, saber defender-se, o menor uso das tecnologias, um bom relacionamento parental e uma boa cultura escolar são fatores protetores na perpetração do *cyberbullying*. Em resposta ao *cyberbullying*, as vítimas consultam muitas vezes amigos ou confrontam-se unilateralmente com os *cyberbullies*, pois não tentam ignorar o problema, contudo, não costumam contar aos pais (Tokunaga, 2010).

Segundo Pedro Verdelho (2016), o facto de a *internet* ser um espaço não regulado e livre, possibilita a que cada um aja da forma que pretender, no entanto, há limites que, ultrapassados, resultam em crime. Existem certos direitos que devem ser assegurados às pessoas que navegam *online*, como o direito a não ser incomodado, insultado, discriminado ou ridicularizado, pois constitui um ilícito criminal (Verdelho, 2016). Nessa conformidade, está também o direito a navegar na *internet* em segurança, isto é, ver apenas aquilo que deliberadamente escolhemos ver, principalmente no contexto mais jovem no que respeita a conteúdos violentos ou pornográficos (Verdelho, 2016), que podem perturbar e até interferir com o normal desenvolvimento da criança. Estes direitos estão expressos na Carta Portuguesa de Direitos Humanos na Era Digital.

3.2. Pornografia infantil

À semelhança do *cyberbullying* também a pornografia infantil já existia antes da *internet*. Contudo, esta veio facilitar a proliferação e acesso ao conteúdo, levantando igualmente algumas questões em relação à sua definição, nomeadamente a dificuldade em tipificar os comportamentos como ilegais e até questões culturais e/ou políticas. O Protocolo Opcional da Convenção sobre os Direitos da Criança de 2002 sobre Venda de Crianças, Prostituição Infantil e Pornografia Infantil define esta última no seu art.º 2, al. c) como qualquer meio capaz de representar uma criança envolvida em atividades sexuais explícitas reais ou simuladas ou a exposição dos órgãos sexuais de crianças para fins primordialmente sexuais. Ly et al. (2018) define pornografia infantil como sendo os " materiais visuais que retratam uma criança num ato sexual e/ou características sexuais da criança" (p. 217). O *International Centre for Missing & Exploited Children* (ICMEC, 2016), de uma forma mais completa, destaca ainda as condutas que levam ao cometimento do abuso: produzir, preparar, consumir, partilhar, divulgar e a posse deste material (Vara & Sani, 2021). Em Portugal é utilizada a designação jurídica "Pornografia de menores" e este crime vem previsto no artigo 176.º do Código Penal. A Interpol, a título de exemplo, adotou a palavra "abuso" em detrimento de "pornografia", recomendando o termo "abuso sexual de crianças", com o intuito de evitar uma associação incorreta com a pornografia de adultos, em que existe o consentimento dos intervenientes (INTERPOL, s.d).

Segundo o FBI, estima-se que o número de indivíduos que procuram conectar-se com crianças em todo o mundo para fins sexuais *online* em qualquer momento chega aos 750 000 (Terre des Hommes, 2018, p.3). A Europol, no seu relatório *Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic* de 2020, reporta a

influência negativa que a pandemia Covid-19 teve no aumento da distribuição *online* de material de abuso sexual de crianças (EUROPOL, 2020d). Em 2019 foram identificadas mais de 3800 vítimas pela *International Child Sexual Exploitation,* uma base de dados da Interpol, sendo que um estudo efetuado em 2018 intitulado *Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material*, identificou que quanto mais nova é a vítima, maior a gravidade do abuso; que 84% das imagens contém atividade sexual explícita; que mais de 60% das vítimas não identificadas eram crianças pequenas e inclusive bebés e que 65% destas eram do sexo feminino; que as imagens de abusos mais graves apresentavam tendencialmente rapazes e ainda que 92% dos ofensores identificados eram do sexo masculino (INTERPOL, 2020b). Relativamente ao perfil das vítimas, o estudo (INTERPOL, 2018) permitiu ainda constatar, além de uma prevalência para o sexo feminino, uma representação muito superior de crianças caucasianas e de crianças em fase de pré-puberdade, não esquecendo que crianças de tenra idade e bebés são também alvo destes abusos. No que aos ofensores diz respeito, importa notar que a sua identificação apenas foi conclusiva em menos de metade dos casos, identificados pela interpol em 2020, existindo uma maioria de caucasianos. Por outro lado, considera-se relevante mencionar um dos desafios identificados no relatório - o facto de os jovens estarem a produzir conteúdo sexual e usando cada vez mais as redes sociais para o distribuir *online* – evidenciando a falta de consciência acerca dos perigos que isso acarreta, pois uma vez na *internet,* para sempre na *internet*. Para além do mais, na circunstância de as imagens, vídeos ou áudios retratarem outras pessoas que não a que disseminou, pode dar-se o caso deste jovem ter querido infligir dor propositadamente, como ato de vingança, ou mesmo que não tenha sido pelas piores razões, os danos podem ser muito graves. Aliás, as redes organizadas de pedófilos recolhem fotografias de crianças e adolescentes, especialmente nas redes sociais, de qualquer tipo, partilhadas por estas ou mesmo pelos progenitores, para posterior venda e difusão na *dark web* (Antunes & Rodrigues, 2018).

De notar ainda dois outros crimes conexos: o *online child sexual exploitation*, que consiste num pagamento ou numa determinada forma de recompensa, por adultos a crianças, para que estas se filmem em direto a praticar atos sexuais (Terre des Hommes, 2018) e o *online grooming* (aliciamento online), em que o adulto procura estabelecer uma relação com a criança para facilitar o posterior contacto sexual *online* ou *offline* (ICMEC, 2016). A PSP tem um papel na consciencialização, no trabalho das informações no que toca à monitorização das redes sociais e à análise do *big data* ("conjunto gigantesco de dados que podem ser recolhidos e analisados computacionalmente, com o objetivo de identificar

padrões, associações e tendências (…).”) (Antunes & Rodrigues, 2018) e, em colaboração com as Escolas, identificar situações de risco.

3.3. Ciberabuso nas relações de intimidade

As TIC constituem um meio facilitador ao desenvolvimento de novos ambientes sociais e, consequentemente, aliciante na criação de novas relações interpessoais, inclusivamente amorosas, sendo que para isso, os jovens têm ao seu dispor uma panóplia de ferramentas digitais (mensagens de texto, chamadas, com recurso à *webcam*, *e-mails*, através das redes sociais, pelo telemóvel, *tablet*, entre outros) (Burke et al., 2011; Borrajo et al., 2015; Caridade & Braga, 2019). Para além da oportunidade de encontrarem velhas amizades e poderem aumentar o seu círculo de amigos à distância de um simples clique, é igualmente arriscada esta forma de socialização, porquanto, a identidade do amigo virtual pode não ser verdadeira (Poiares, 2020). Mencionar também que aquelas podem provocar uma maior suscetibilidade à intrusão interpessoal dos jovens e crianças, levando a fenómenos de vitimação como o *cyberbullying*, o *cyberstalking*, o *sexting* ou o *cyber dating abuse* (Caridade et al., 2020).

O ciberabuso pode ser definido como uma forma de controlo, assédio e perseguição do/a parceiro/a amoroso/a, através da tecnologia e dos meios de comunicação social (Zweig et al., 2013a), podendo assumir múltiplos comportamentos abusivos, desde o controlo e vigilância diária do parceiro ou ex-parceiro; a publicação de comentários ofensivos ou humilhantes para o parceiro; o envio de mensagens ameaçadoras; a publicação de fotografias ou o envio de vídeos pelas redes sociais com a finalidade de humilhar ou prejudicar o parceiro; a utilização das contas pessoais do parceiro sem a sua autorização para o espiar, entre outros (Borrajo et al., 2015; Caridade & Braga, 2019). Ao contrário do mundo *offline*, as vítimas no ciberespaço experienciam este tipo de condutas de forma imediata, assíncrona e na ausência de limites espácio-temporais (a qualquer momento e a partir de qualquer lugar) (Vale et al., 2021).

No estudo de Zweig et al. (2013b) verificou-se uma taxa de vitimação dos adolescentes de 26% e que mais de 1 em 10 jovens numa relação (12%) poderão perpetrar este tipo de abuso. Os mesmos autores noutro estudo constataram uma forte correlação entre o ciberabuso e a prevalência de sintomas depressivos, possuir níveis elevados de raiva/hostilidade, cometer mais atos de delinquência, ter uma vida sexual ativa e ser mulher, no entanto, não se determinou se correspondem a fatores de risco ou se são consequências da vitimação (Zweig et al., 2013a). Relativamente ao género, concluíram que a mulher, não

só apresentava um nível de vitimação superior, mas também era a que cometia mais estes atos (Zweig et al., 2013a; Villora et al., 2019). Nesta conformidade, níveis elevados de comportamento ciumento e de hostilidade demonstraram ser preditores do ciberabuso no namoro, como evidenciou também o estudo de Deans e Bhogal (2017). Estes autores, pelo contrário, no que toca ao género notaram que as mulheres reportavam níveis inferiores de perpetração. Villora et al. (2019) inferiram que a dependência emocional, a negatividade dos apegos, uma maior competência digital e a falta de apoio social são características comuns às vítimas e perpetradores. Contudo, em outros estudos realizados, encontram-se resultados díspares quanto à caracterização do perfil daqueles. Numa investigação a nível nacional (n= 4938, entre 11 e 20 anos), 21% dos inquiridos reportaram terem sido vitimados pelo parceiro nas redes sociais, sendo a forma de perpetração mais frequente aceder à conta sem a autorização do titular (UMAR, 2019).

Como sustentam Vale et al. (2021) tem de existir um comprometimento entre 3 setores: adolescentes, família e sociedade, pois "a segurança na *internet* é também segurança emocional" (CIS, 2022, para. 3). Nesse âmbito, é de assinalar algumas iniciativas importantes na reflexão e eliminação destas práticas limitadoras, abusivas e agressivas, como foi o caso da campanha "Violência no Namoro Online" desenvolvida pelo Centro *Internet* Segura no dia 4 de fevereiro de 2022, para assinalar o Dia da *Internet* mais segura (8 de fevereiro) (CIS, 2022); a Campanha de Filipe Meunier e a APAV "A violência *online* é real", em 2021; a campanha *online* "#GrrEudigoNãoaoCiberabusonoNamoro" a nível regional; as várias campanhas da Escola Segura (*Internet mais Segura*) nas escolas durante todo o ano letivo; a criação de uma aplicação para telemóvel pela Universidade do Minho, denominada "#CiberAmigo", ganhadora de um prémio e possível ferramenta a ser utilizada nas escolas (Lusa, 2020b). Esta *app* permite obter informação acerca da ciberagressão e as suas dinâmicas, sobre as *fake news*, em que o objetivo é desconstruir (ciber)mitos que estejam a legitimar determinados comportamentos e ainda garante uma resposta efetiva aos pedidos de ajuda e denúncias por parte das crianças e adolescentes, encorajando à denúncia e prevenindo a divulgação nas redes sociais (Lusa, 2020b). Apesar das várias campanhas realizadas pela PSP sobre violência no namoro, ainda não se direcionam muito para o espaço ciber, não esquecendo o Programa Comunicar em Segurança em parceria com a MEO e a Fundação Altice, em que são publicados nas redes sociais vários conselhos e informação relevante sobre várias temáticas, incluindo esta.

Por sua vez, os pais devem procurar estar atentos e disponíveis, pois a adolescência é uma fase complicada, nomeadamente participando nas práticas *online* dos seus educandos,

estimulando o diálogo com eles e incutindo bons valores, enquanto as escolas podem adotar medidas como: rever o currículo pedagógico e integrar a componente da literacia digital a partir do primeiro ciclo; realizar aulas de cidadania, ações de sensibilização e/ou palestras, consciencializando para a natureza, dinâmicas e consequências destas ações; "desconstruir crenças disfuncionais sobre o amor/controlo e sobre as representações da violência e a sua tolerância e estimular o papel interventivo dos ciberobservadores"; adotar estratégias de prevenção e intervenção (Vale et al., 2021, p. 128).

3.4. *Cyberstalking*

O *cyberstalking* é outra forma de violência *online* e de intrusão interpessoal. Comparativamente com o *cyberbullying*, que ocorre máxime no contexto escolar e em camadas mais jovens, a prevalência aqui abrange os adolescentes, jovens adultos e os adultos, mas pode ser transversal a qualquer idade. Das várias definições encontradas, destaca-se: a procura repetida de uma pessoa por outra utilizando as TIC, provocando nesta uma resposta emocional grande ou o sentimento de medo pela sua segurança ou de alguém próximo (Fissel & Reyns, 2019). Assim têm de existir cumulativamente as seguintes condições: estar perante um evento repetido, o direito razoável da pessoa à sua privacidade tem de ser violado e a existência de ameaça evidente e o facto de esta não ser dirigida unicamente à vítima, podendo englobar a sua propriedade ou as redes sociais (Dhillon & Smith, 2017). Os comportamentos mais frequentes passam por fazer chamadas, enviar *e-mails* e mensagens escritas por telemóvel, contudo, a gravidade pode aumentar para a realização de chamadas ou mensagens com conteúdo obsceno ou ameaçador, a invasão da propriedade da vítima e a espionagem das suas atividades e comunicações (Sani et al., 2018). Os autores definiram uma escala dos comportamentos dos *ciberstalkers* de acordo com o grau de ameaça que causam na vítima: hiperintimidade, sabotagem, ameaça e transferência para a vida real. Em similitude com o que ocorre nas outras formas de violência descritas anteriormente, o agressor consegue, sem estar perto da vítima, prejudicar e invadir a sua privacidade, assim como tem a capacidade de persuadir terceiros a intimidar ou ameaçar a vítima (Sani et al., 2018).

Num estudo realizado por Sani e Valquaresma (2020), verificou-se que 68% dos estudantes do ensino secundário (n=259) experienciaram pelo menos um comportamento de *cyberstalking* e que os homens são mais vitimados por comportamentos de ameaça do que as mulheres. No que toca ao género, March et al. (2020) concluíram que as mulheres perpetuam mais este tipo de condutas, contrariamente ao que acontece com o *stalking*, sendo

a insegurança e a necessidade de evitar a rejeição fatores preditivos. Outro destes fatores é a predisposição para comportamentos de controlo face ao parceiro numa relação (March et al., 2020; Todd et al., 2020). Logicamente que esta correlação é quase certa, pois o *stalker* pretende obter uma reação ou atitude nova ou diferente das anteriores por parte da vítima, que lhe convém, e tal pode acontecer durante o relacionamento ou posteriormente. Muitas das vezes a vítima não percebe que está numa relação abusiva e inclusive aceita e defende o agressor, sendo certo que estas condutas podem configurar o crime de violência doméstica (Poiares, 2020) e escalar até ao homicídio, como indicou o estudo de Todd et al. (2020). Daí que o *cyberstalking* esteja muitas vezes ligado ao ciberabuso nas relações de intimidade. Contudo, apesar da maior parte dos estudos focarem-se nestes comportamentos no seio de uma relação, o ciberespaço possibilita que sejam cometidos por completos estranhos (Marcum et al., 2017).

A monitorização do ciberespaço permite, através das pegadas digitais, identificar vítimas e perpetradores (as suas motivações e *modus operandi*) e concomitantemente prevenir o agravamento das condutas, especialmente a sua transferência para o mundo *offline*. No estudo de O´Shea et al. (2019), algumas das dificuldades referidas pelos polícias foram a dependência das tecnologias por pessoas cada vez mais jovens e a sua especialização, não conseguindo atuar perante tanta informação; o anonimato e o consequente impedimento na descoberta do autor do crime e ainda as constantes novas técnicas utilizadas pelos *cyberstalkers*.

3.5. Dependência *online*

Há estudos que indicam que a média de idades com que os jovens começam a utilizar a *internet* é de 8 anos (Patrão et al., 2012), porém é possível observar e é sabido que, atualmente, crianças ainda mais novas já têm contacto com as TIC. Na investigação referida, concluíram que aqueles passam em média 6 horas diárias *online* para atividades de lazer, sendo as atividades preferenciais as redes sociais (62,2%), a multimédia (ex: *youtube*, filmes ou séries) (23,9%) e os videojogos (16,2%). Segundo os próprios, as horas que passam na *internet* retira-lhes tempo para outras atividades como estar em família, dormir, fazer exercício físico, ter atividades lúdicas (*offline*) e para a escola, considerando-se dependentes do que fazem *online* (69,9% de n= 259) (Patrão et al., 2012). De notar que se trata de uma amostra de jovens com um uso problemático da *internet*.

Num inquérito realizado pelo SICAD (2019) aos participantes no Dia da Defesa Nacional, os problemas mais mencionados, associados à utilização da *internet*, respeitam ao

rendimento na escola/trabalho, a situações de mal-estar emocional e problemas com comportamentos em casa. Lemos (2019, p. 34) identificou que o UPI e das redes sociais correlacionam-se negativamente com a saúde mental, o bem-estar psicológico e positivamente com a sintomatologia e o "*distress*" psicológico. Ou seja, a autora refere que a utilização das plataformas digitais não permite a satisfação das necessidades psicológicas e origina consequências negativas e sintomas psicopatológicos. De outro prisma, é possível analisar que quem já tem este tipo de problemas mentais é atraído para estas plataformas, como uma forma de se isolar e até sentir bem-estar, desencadeando o seu uso dependente e desadequado (Kuss & Griffiths, 2011; Patrão et al., 2012).

Alguém é considerado dependente quando se reúnem 6 critérios: quando a atividade *online* se sobrepõe a tudo o resto (necessidades básicas, rotinas, etc.); quando a *internet* é utilizada para lidar com os estados emocionais que surgem; ou para colmatar a necessidade de obter satisfação; quando ocorrem sintomas derivados da privação; quando a pessoa demonstra dificuldades interpessoais e relacionais e de nível académico e/ou ocupacional e a recaída após períodos de controlo relativo (Patrão, 2019).

3.6. Consequências da cibervitimação em crianças e jovens

O impacto do cibercrime na vítima varia de acordo com diferentes aspetos, podendo-se agravar ou atenuar, desde logo devido às suas características sociodemográficas e às competências digitais que possui; depois, pelo tipo de crime a que foi sujeita e o nível de agressão subjacente; também a sua duração, o tamanho da audiência e a relação com o autor do cibercrime (quando se aplica) e ainda a existência ou não de uma rede de suporte (APAV, 2019). Durante a pandemia as crianças viram-se obrigadas a ficar confinadas em casa, o que trouxe desafios a nível *online* mas igualmente *offline*, incluindo isolamento social, ausência de apoio por parte dos pares, professores e demais cuidadores, aumento do tempo despendido *online*, ansiedade, *stress*, entre outros impactos na saúde mental (Europol, 2020d).

Os poucos estudos que abordam este tópico são predominantemente focados em determinadas formas de cibercrime. Segundo a APAV (2019), as consequências experienciadas pelas vítimas de crimes cibernéticos não diferem em grande medida das vivenciadas por vítimas de crimes tradicionais. As mais assinaladas são: depressão, ansiedade, perda de autoconfiança e confiança nos demais, problemas de concentração, dificuldade em dormir, medo, culpa, vergonha, humilhação, tristeza, sentimento de solidão, dificuldades interrelacionais, problemas socio-emocionais e menor desempenho escolar (Betts, 2016; Jansen & Leukfeldt, 2017; Worsley et al., 2017; Zilka, 2017; Gewirtz-Meydan

et al., 2018). Mais concretamente, no caso do *cyberbullying*, elenca-se o sofrimento, a tristeza, a solidão, a baixa autoestima, a raiva, a frustração e ainda a depressão e a ideação suicida (APAV, 2019). Para além da correlação positiva com comportamentos suicidas, observa-se uma associação com o consumo de substâncias e o comportamento violento e sexual (Litwiller & Brausch, 2013). No *cyberstalking*, o medo poderá dirigir-se ao ator dos atos, mas também devido à perda da reputação e pela possibilidade de informações pessoais e privadas ficarem expostas *online* (APAV, 2019). Já no ciberabuso, as vítimas poderão sentir culpa e vergonha, medo, confusão, raiva, solidão, ansiedade e insegurança (Apavparajovens, s.d). O impacto do abuso e exploração sexual no desenvolvimento de crianças e adolescentes acontece pela própria experiência desse abuso, mas também pela partilha e visualização repetidas desses conteúdos (Vara & Sani, 2021). A dependência das tecnologias pode ter impacto na saúde, primordialmente na infância e adolescência, dado que são períodos críticos no desenvolvimento da pessoa, quer a nível físico (e.g. alterações na postura, grande oscilação no peso), psicológico (e.g. alterações no humor, nas rotinas de sono) e social (e.g. dificuldades na socialização e no processo de autonomia emocional e económica) (Patrão, 2019).

Em suma, é percetível que as crianças e os jovens são grupos etários bastante vitimados por este tipo de comportamentos, que muitas das vezes, devido ao seu excesso de confiança, são por estes subvalorizados. A educação é a primordial arma para a prevenção, não obstante, a avaliação dos fatores de risco e fatores preditivos, a aplicação de mecanismos de proteção e acompanhamento das vítimas e medidas de controlo, punição e tratamento dos agressores (Sani et al., 2018) são cruciais no seu combate.

3.7. A cibereducação como medida preventiva no combate ao cibercrime

De acordo com o *Relatório Cibersegurança em Portugal-Sociedade 2021*, Portugal apresenta alguns valores abaixo da União Europeia, no que às atitudes e comportamentos e educação diz respeito. Em particular, os portugueses tendem a ter menos cuidados de segurança com o *smarthphone*, possuem menor conhecimento e cuidado em relação à função e uso dos *cookies* e utilizam mais as redes sociais (CNCS, 2021d).

Em ordem a prevenir e combater o cibercrime, primeiro que tudo, há que estar informado, conhecer o fenómeno, os perigos, as vulnerabilidades, os perfis dos autores dos crimes, os seus *modus operandi*, o tipo de ilícito e por conseguinte o tipo de vítima correspondente. Em segundo lugar, é preciso tomar medidas e estar protegido *online* e ao nível da "Internet das Coisas", o que implica igualmente que haja um nível de literacia digital

básico. Quando se tratam de crianças, os pais devem pugnar por esse conhecimento, para o poderem transmitir, assim como proteger a criança contra potenciais riscos. Em terceiro lugar, importa perceber a utilidade da denúncia em termos de IC e prossecução da justiça, pelo que o caminho nunca é o silêncio ou o isolamento.

Santos, Bessa e Pimentel (2008), Carvalho e Marques (2017) e Robalo (2021) defendem que o caminho a seguir, em relação ao cibercrime, é o da prevenção, cuidado e informação, pois como argumentam os primeiros "a segurança total é inatingível" (p.201). Segundo o Portal da Queixa (2022), num estudo realizado sobre Segurança Online, 55,2% dos consumidores portugueses inquiridos já foram alvo de tentativa de burla *online*, enquanto 33,6% foram efetivamente vitimados por este crime. Nesta investigação concluiu-se que o nível de literacia digital dos portugueses é baixo, há pouco conhecimento acerca dos tipos de ataques cibernéticos e as medidas de proteção adotadas são escassas e fracas (Portal da Queixa, 2022). Carvalho e Marques (2017) defendem que a prevenção é necessária para a deteção, evitamento e combate dos efeitos do cibercrime, sendo alcançada com a aposta no desenvolvimento tecnológico e na formação dos utilizadores. Sustentam ainda que a formação deve ser ministrada logo no ensino básico e secundário, já que se tornam consumidores das novas tecnologias desde muito cedo, designadamente no que respeita aos riscos da sua utilização, vulnerabilidades dos sistemas e medidas de prevenção a implementar para os minimizar (Carvalho & Marques, 2017).

Um sítio na *internet* apetecível para os jovens é as redes sociais, em que se podem encontrar desafios ao nível da segurança, da privacidade dos dados e dos seus utilizadores (Antunes & Rodrigues, 2018). A sua utilização não encontra uma barreira etária, porquanto, apesar de haver restrições aquando a criação de uma conta, é fácil contornar esse facto, e por isso, muitos são os utilizadores do *Facebook*, por exemplo, com menos de 13 anos de idade (Antunes & Rodrigues, 2018). Assim, os autores ressaltam a necessidade de formar e educar conscientemente os utilizadores das redes sociais, em especial as crianças desde tenra idade, nomeadamente no que concerne à partilha de conteúdos e à eficiente configuração e gestão dos perfis de utilização.

São possíveis intervenientes na cibereducação dos cidadãos: o CNCS, as empresas privadas, a comunicação social, as escolas, os pais/cuidadores e as Forças de Segurança. A PSP, para além das ações de sensibilização, palestras, ações de formação, partilha de informação nas plataformas digitais direcionada para todos os públicos-alvo, tipos de crime e demais conteúdo relevante (um "kit de materiais"), jogos interativos, quiz´s, campanhas e ferramentas de ciberhigiene e ciberdefesa, também deve atuar no seio escolar, através do

mencionado, mas ainda na deteção e intervenção precoce em situações de *cyberbullying* e outras problemáticas que ocorrem por via *online*, em colaboração com os professores e assistentes operacionais. Ao nível da dissuasão de potenciais cibercriminosos, têm igualmente de existir ferramentas, como o Projeto "EMPACT". Sustenta-se a existência de reuniões periódicas entre os polícias afetos à Escola Segura e os professores e assistentes operacionais, que são quem tem mais contacto com as crianças e jovens; também a criação de círculos de conversação nas escolas sem e com a presença de um polícia do MIPP; podia haver inclusive uma aula integrada no plano curricular lecionada por um polícia, com a difusão de conteúdos dinamizadores, com a criação de projetos de ajuda entre pares (Thompson & Smith, p.247), no fundo envolver os estudantes no tema da cibersegurança. Desta forma, é preciso que os polícias do MIPP tenham formação nesta área, para ensinar e educar os demais ou até quem sabe, criar aplicações para os dispositivos móveis. A família é outro ator crucial, enquanto agente de socialização e peça chave no desenvolvimento da criança, dado que o estilo educativo incutido pode influenciar o rendimento académico, a autoestima e/ou as competências psicossociais e de aceitação social dos pares (Yubero et al., 2013). As particularidades do ciberespaço condicionam a ação dos pais a nível do controlo e supervisão, possuindo apenas um papel de mediador no uso das TIC e na comunicação, como constatam os autores. No entanto, como afirma Guinote (2021), "os pais passam a assumir o papel de colegas na resolução de conflitos", quer internos, quer externos como o *cyberbullying*. Em suma, "a segurança não é uma questão técnica apenas, mas também, uma questão estratégica e humana" (Tribolet, as cited in Santos et al., 2008, p. 228).

Capítulo 4: Opções metodológicas e resultados

4.1. Opções metodológicas

O início de uma investigação exige método, pelo que implica seguir várias etapas de um procedimento com rigor, porém tal não significa rigidez e sim flexibilidade e adaptação (Campenhoudt et al., 2019). "Método é o conjunto das atividades sistemáticas e racionais (…) que permite produzir conhecimentos válidos e verdadeiros" (Marconi & Lakatos, 2017, p. 91), mediante o planeamento e a aplicação de uma ou mais técnicas (Santo, 2015).

Após a definição da pergunta de partida, a exploração, a identificação dos objetivos, em particular perceber o papel da PSP na prevenção do cibercrime, examinar o papel do MIPP na cibersegurança, conhecer o grau de conhecimento de EE em relação ao risco que os educandos correm ao navegar na *internet* e analisar o impacto da cibervitimação nas

camadas mais jovens, cabe agora explicar as opções metodológicas escolhidas e o trabalho empírico realizado.

No que à realização deste trabalho diz respeito, procurou-se examinar o fenómeno da cibersegurança e consequentemente do cibercrime, em especial, a caracterização do ciberespaço, dos ofensores e das vítimas. Também foi analisado o policiamento de proximidade e a sua adaptação ao contexto em estudo e ainda examinado o nível de vitimação cibernética de crianças e jovens. Para atingir estes objetivos, procedeu-se à revisão da literatura existente, que permitiu aprofundar o conhecimento acerca das temáticas em estudo. A abordagem adotada foi mista, por um lado, qualitativa, optando-se pela técnica da entrevista e, por outro, quantitativa, mediante a aplicação de um inquérito por questionário e conjugando-se e concluindo-se com base nos resultados integrados das técnicas utilizadas.

A entrevista porque se trata de uma "técnica de recolha de dados em profundidade e em que se privilegia a qualidade da informação, valendo as respostas de cada indivíduo por si mesmas" (Santo, 2015, p.33). Com vista a identificar o grau de conhecimento dos pais/encarregados de educação de crianças a frequentar o primeiro ciclo do ensino básico em relação à exposição dos seus filhos/educandos à *internet*, realizou-se um inquérito por questionário a crianças com idades compreendidas entre os seis e os dez anos. A aplicação deste inquérito surgiu pela tendência de a utilização dos meios tecnológicos ser feita numa idade, cada vez mais, precoce (Ofcom, 2020) e na impossibilidade de realizarem inquérito, terem de responder os pais/EE. Para além disso, constatou-se, através do estado da arte, que uma lacuna, será a não consideração das crianças mais jovens (Dias & Brito, 2021), como são exemplo: Cepeda, 2012; Costa, 2014; Paulus et al., 2018; Asam et al., 2019; SICAD, 2019; Ponte et al., 2020, entre muitos outros cujo universo são adolescentes ou crianças com idade a partir dos nove anos.

Os informadores qualificados foram previamente elucidados acerca dos objetivos da realização da entrevista e questionados sobre o seu consentimento face à utilização do recurso áudio e à citação da sua identidade (Apêndice B). A aplicação das entrevistas foi precedida de autorização por parte da Direção Nacional da PSP, que consta no apêndice C. No que concerne aos inquéritos, ambos os Agrupamentos de Escolas autorizaram a sua aplicação na respetiva escola (cfr. Apêndices D e E). A recolha de dados na escola no Município do Cartaxo foi a 25 de março de 2022, enquanto na escola do Município de Odivelas foi a 06 de abril do mesmo ano.

As dificuldades sentidas foram a ausência de colaboração por parte de informadores externos à PSP, pese embora a repetida insistência, a morosidade em aplicar o inquérito nas

escolas e a respetiva resposta por parte dos EE, a que acresce o pouco cuidado no seu preenchimento, com várias questões em branco. Perante a primeira dificuldade, a autora teve de fazer escolhas e cingir-se aos principais objetivos do trabalho, resultando apenas as entrevistas aos polícias. Respeitando aos inquéritos, através de telefonemas e mensagens de correio eletrónico, foi possível chegar às escolas que possuíam o maior número de alunos naqueles municípios. Seguidamente, com idas às escolas para falar com os responsáveis, obteve-se a autorização e o número de turmas e alunos por turma para facilitar a entrega dos inquéritos.

4.2. Trabalho empírico: instrumentos de recolha de dados

4.2.1. Entrevistas: o papel da PSP na prevenção do cibercrime

A realização das entrevistas prendeu-se com três objetivos: examinar o papel da PSP na prevenção e no combate ao cibercrime, uma vez que era necessário perceber como os crimes cometidos com recurso às TIC são da competência exclusiva da PJ; analisar a possibilidade de "patrulhar" o ciberespaço e como é/poderá ser feito e ainda verificar a adaptação do policiamento de proximidade ao ciberespaço e como fazê-lo.

As entrevistas são semiestruturadas, a partir de um guião previamente concebido (apêndice F), porém com a possibilidade do entrevistador conduzir a conversa de acordo com os objetivos traçados. Para este estudo foram escolhidos seis polícias, dois Oficiais e um Agente Principal com trabalho produzido nesta área e outros três Oficiais cujas funções que desempenham poderiam permitir contribuir para o alcance dos objetivos supramencionados. As entrevistas decorreram individualmente, de forma presencial ou via *zoom*, entre os dias 1 e 17 de fevereiro de 2022, com recurso a registo áudio após a autorização dos entrevistados, terminando na sua ulterior transcrição, que se encontra no apêndice G.

No sentido de categorizar os dados resultantes das entrevistas, conferindo-lhes organização e sentido (Sarmento, 2013), para se poder melhor interpretar e procurar compreender criticamente o sentido por detrás das palavras do entrevistado (Bardin, 2016; Severino, 2017), utilizou-se a técnica de análise de conteúdo. A análise de conteúdo permite sistematizar a informação, através de processos de codificação, categorização e inferência (Santo, 2015). Na codificação, procede-se a três operações: a escolha das unidades, a escolha da regra de contagem e a escolha das categorias, em ordem a efetuar o processo de categorização (Santo, 2015; Bardin, 2016).

Através da análise de conteúdo foi possível sistematizar e organizar os dados decorrentes das entrevistas aplicadas aos diversos informadores qualificados, no campo da atuação policial e no plano das vítimas. Primeiramente, examinou-se cada resposta do *corpus*, realçando-se os excertos mais pertinentes para a questão e de seguida, elaboraram-se as matrizes cromáticas das unidades de contexto e de registo das várias perguntas, em que se identificam as partes que os informadores mais valorizam, salientando-se as partes semelhantes, tendo este processo resultado na codificação das unidades de registo. Em segundo lugar, com base nas matrizes já efetuadas, procedeu-se à análise categorial. Para tal, determinou-se as categorias, as subcategorias, incorporou-se as unidades de registo previamente estabelecidas, as unidades de enumeração e calculou-se a respetiva frequência absoluta, resultando nas matrizes de registo da análise de conteúdo. O quadro categorial construído obedece a alguns princípios postulados por Bardin (2016), como cada categoria ser única em cada divisão ("papel da PSP na prevenção e no combate ao cibercrime", "reforço da capacidade de investigação destes crimes", "monitorização do ciberespaço", "especificidades a ter em conta na monitorização do ciberespaço", "controlo *online*", "MIPP", "público-alvo a apostar", "riscos que correm as crianças ao navegar na *internet*" e "desafios da cibercriminalidade no futuro"), fornecendo hipóteses novas e permitindo diferentes inferências, cada unidade de registo existir apenas numa subcategoria e as unidades de registo adequarem-se aos objetivos da análise.

4.2.2. Inquérito por questionário: O grau de conhecimento de 520 EE acerca da exposição dos seus educandos à *internet*

A utilização da técnica do inquérito permite não só, analisar estatisticamente um fenómeno, como possibilita averiguar a relação entre as variáveis que sejam pertinentes (Stockemer, 2019). A informação recolhida por meio de inquérito, pelo facto de ser sintética e não aprofundada, é suscetível de ser categorizada de forma padronizada (Santo, 2015). Outra vantagem desta técnica é a possível comparação e generalização dos resultados decorrentes da sua aplicação (Santo, 2015).

No sentido de apurar o nível de conhecimento de pais/EE sobre os riscos que correm os seus filhos/educandos com a utilização dos meios eletrónicos, o inquérito foi aplicado em duas escolas do ensino básico de cidades com população e território muito distintos: Cartaxo, que apesar de ser uma cidade, é mais rural e Odivelas, uma cidade do distrito de Lisboa. Entre elas existe uma diferença de 36417 pessoas, com 23187 (total das freguesias) e 59604 (freguesia de Odivelas) respetivamente, segundo os Censos de 2021 (INE, 2021). O Cartaxo

alberga uma área de 158,17 km² e Odivelas apenas 26,54 km². A Escola Básica José Tagarro no Cartaxo possuía à data 294 alunos enquanto a Escola Básica Manuel Coco em Odivelas contava com 362 alunos, perfazendo uma população de 656 EE. A amostra consistiu em 528 EE de crianças entre os 6 e os 12 anos de idade. Contudo, os valores omissos das variáveis sociodemográficas foram excluídos, não sendo úteis para o estudo, pelo que a amostra reduziu para 520 respostas e uma taxa de resposta de aproximadamente 79%. A amostra é do tipo probabilístico dado que tem por base uma lista completa e atual de todos os membros que constituem o universo e tratou-se de um inquérito aplicado por via de um conjunto de elementos informados sobre o âmbito do estudo, que entregaram e recolheram o inquérito junto dos educandos, os quais serviram de mediadores junto dos seus EE. Com base no universo (656) e na amostra (520) obtida, após validação dos inquéritos e considerando um nível de confiança de 95%, resultou o erro de amostragem para populações finitas em aproximadamente 1,97%. Foi utilizada a fórmula de cálculo: E= $Z \times \sqrt{\frac{N-n}{N} \times \frac{pq}{n}}$ (Spiegel & Stephens, 2009).

Cada inquérito é composto por quatro variáveis sociodemográficas (idade, sexo e ano de escolaridade da criança e habilitações literárias do EE), mais 11 variáveis hipoteticamente dependentes (frequência com que a criança está *online* ou usa a *internet* por dispositivo eletrónico; tempo que a criança despende sozinha na *internet* por dia de semana e por dia de fim de semana; atividades que a criança mais pratica nos tempos livres; alterações comportamentais da criança face à exposição às TIC; situações que aconteceram à criança nos últimos doze meses; atuação do EE perante essas situações; resposta das autoridades; cuidados do EE no acesso da criança à *internet*; ação do EE quando a criança está *online*; situações na escola com a criança e EE que aconteceram nos últimos doze meses e medidas a adotar na escola), sendo a última com uma alínea de resposta aberta (Apêndice H). Esta última variável foi introduzida com o intuito de "complementar e contextualizar a informação quantitativa obtida pelas outras variáveis" (Hill & Hill, 2016, p.95). O inquérito contém variáveis adaptadas do inquérito europeu *EU Kids Online* de 2018 (1ª, 2ª, 3ª, 5ª e 9ª perguntas fechadas), que teve aprovação da Comissão Nacional de Proteção de Dados (Ponte et al., 2020), e variáveis construídas para este estudo de forma a poder-se responder aos objetivos de investigação formulados. Utilizou-se aquele inquérito no sentido de estudar a relação de crianças com a *internet*, neste caso, pela visão dos EE e não das próprias crianças.

Realizou-se ainda um pré-teste na Escola José Tagarro no Cartaxo a 15 EE, contando a versão final após revisão por especialista[4] e a testagem do inquérito.

A técnica do inquérito por questionário serve para "descrever uma população" (Reis, 2018, p.99), neste caso as crianças do 1.º ao 4.º ano de escolaridade das duas escolas assinaladas, face ao fenómeno em estudo, a cibersegurança, relacionando neste caso as variáveis: idade, frequência nos dispositivos digitais, tempo passado na *internet* sozinha, as atividades praticadas nos tempos livres, alterações comportamentais, situações de risco, cuidados de acesso, situações com a escola e EE e medidas de segurança a concretizar na escola. Não obstante, essa descrição é conseguida através do grau de conhecimento que os EE têm dos seus educandos, o que permite igualmente aferir algumas considerações, referidas infra, daí o objetivo da aplicação deste instrumento de análise.

O tratamento e a análise estatística dos dados recolhidos foi efetuada através do *software* informático *Statistical Package for the Social Sciences* (SPSS) versão 27. Inicialmente, realizaram-se apuramentos simples para todas as variáveis e posteriormente efetuaram-se cruzamentos e respetivo teste de qui-quadrado.

4.3. Apresentação de resultados

4.3.1. Análise de conteúdo das Entrevistas[5]

Analisando a primeira questão: No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime? (quadro 1 do apêndice I) – Relativamente à prevenção, metade dos informadores qualificados afirmam que a PSP possui um papel fundamental nesta vertente de atuação contra o cibercrime; 83% destacam a necessidade de esclarecimento e consciencialização da população; apenas 17% mencionam a cooperação, mais precisamente no âmbito do Projeto Comunicar em Segurança, como forma de assegurar a cibersegurança e prevenir a cibervitimação; 17% indicam dois pilares que devem fazer parte desta vertente: as políticas de intervenção e a divulgação e ainda 17% declaram haver ainda um caminho a percorrer nesta área. No que ao combate diz respeito, 33% são da opinião de que a PSP tem aqui uma intervenção secundária apenas, contrariamente, 17% acreditam ter uma contribuição importante. Dois informadores defendem essa contribuição a nível da sinalização de situações que configurem crimes ou atividades que possam parecer atos preparatórios da sua prática, porém um declara que é algo que ainda não está a ser feito. Na mesma proporção, é argumentado de que a vertente

[4] Paula do Espírito Santo, na qualidade de orientadora e especialista na área de métodos.
[5] Os quadros referentes à análise de conteúdo das entrevistas encontram-se no Apêndice I.

do combate está afeta ao Núcleo de Cibercriminalidade exclusivamente. Por último, 17% afirmam que a PSP atua nas duas vertentes, dando apoio à estrutura de investigação criminal no âmbito da prevenção, deteção e investigação deste tipo de crimes, fornecendo formação ao efetivo que compõe o Núcleo de Cibercriminalidade e ainda monitorizando fontes abertas e emitindo alertas operacionais (33%) e um entrevistado refere que o papel da PSP, na vertente do combate, se circunscreve aos crimes ciber-instrumentais. Para melhor compreensão da análise, apresenta-se o quadro n.º 1 infra, com a categorização desta questão.

Quadro 1- Categorização da questão n.º1: "No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?"

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Papel da PSP na prevenção e no combate ao cibercrime	Prevenção	1.1. Papel fundamental	X			X		X	3	50%
		1.2. Esclarecimento e consciencialização das pessoas	X	X	X		X	X	5	83,3%
		1.7. Políticas de intervenção e divulgação a nível do policiamento de primeira linha			X				1	16,7%
		1.11. Caminho a percorrer ainda					X		1	16,7%
		1.12. Cooperação					X		1	16,7%
	Combate	1.3. Papel secundário	X			X			2	33,3%
		1.8. Sinalizar situações e investigá-las			X			X	2	33,3%
		1.9. Sediado no Núcleo de Cibercriminalidade				X	X		2	33,3%
		1.13. Missão importante						X	1	16,7%
	Ambos	1.4. Papel nos crimes ciber-instrumentais		X					1	16,7%
		1.5. Dar apoio à estrutura de IC no âmbito da prevenção, deteção e investigação deste tipo de crimes		X	X				2	33,3%
		1.6. Monitorização de fontes abertas e realização de alertas operacionais		X	X				2	33,3%
		1.10. Ação nas duas áreas, prevenção e combate						X	1	16,7%

Procedendo à análise da segunda questão: Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital? – Os informadores referem 5 principais fatores (quadro 4) que contribuem para melhorar a capacidade investigatória da PSP, sendo os mais citados a formação e especialização do efetivo policial (80%); a cooperação (60%), nomeadamente com o setor privado, as operadoras telefónicas, com o mundo académico e científico, lembrando o Chefe do NAOP (Inf 3) que a responsabilidade da PSP neste domínio não é consensual (quadro 3) e ainda a necessidade de haver meios técnicos (40%), a par com os conhecimentos técnicos e a formação, meios esses que carecem de alguma sofisticação e especialidade, devido à evolução das TIC. Para além dessas, foi mencionada ainda a importância da atividade de monitorização do ciberespaço, em especial das redes sociais, a sensibilização para uma cultura de denúncia dos crimes e a sinalização de práticas criminais, todas com 17% (quadro 4). Dos informadores, 60% admitiram a falta de capacidade da PSP para atuar nesta dimensão do combate/investigação criminal neste tipo de criminalidade, sinalizando falhas como a escassez de efetivo, ausência de ferramentas devido à fraca possibilidade económica e ausência de *know-how*, sendo o especialista em cibersegurança (Inf 4) da opinião de que a ação da PSP se deve circunscrever à prevenção (quadros 3 e 4).

Respeitante à questão três: Como se adaptou o policiamento tradicional a um espaço não físico e como se "patrulha" o ciberespaço? – Verifica-se, através do quadro 6, várias tendências nas quatro subcategorias definidas: primeiro, 50% referem que existe um trabalho de monitorização do ciberespaço no Núcleo de Cibercriminalidade e não só, porém é feito de forma direcionada, isto é, no âmbito de um processo ou para seguir um fenómeno (quadro 5) e apenas um informador acredita que esta atividade é desenvolvida somente no âmbito das Informações (17%), porquanto "eu não diria que neste momento nós fazemos um patrulhamento do ciberespaço, o que nós fazemos é trabalhar a fase pré-crime" (quadro 5). Apenas 33% assinalam a importância de o ciberespaço ser alvo de uma monitorização recorrente, destacando o Oficial de Ligação da PSP (Inf 6) o trabalho desenvolvido no âmbito da prevenção da violência no desporto (quadro 5). No que toca à adaptação, foram fornecidas as seguintes ideias: necessidade de capacidade técnica dos investigadores por 33% para se conseguir de facto adaptar; existência de alertas, por 17% no sentido de haver uma espécie de "presença" da Polícia no ciberespaço; o policiamento tradicional e o policiamento no ciberespaço assumem os mesmos contornos (17%), isto no que concerne à prevenção feita no âmbito do MIPP, em que o Coordenador do PP (Inf 5), menciona "é baseado na relação de confiança que os agentes vão estabelecendo com os alunos, em que, pontualmente vão interagindo com eles no espaço virtual (…) (quadro 5) "; cultura de

denúncia do crime e partilha de prova (17%), desta vez focalizada nos alunos (quadro 5); existência de uma boa adaptação do policiamento tradicional ao ciberespaço (17%) igualmente na vertente do policiamento de proximidade, com o desenvolvimento de "muitos conteúdos formativos e de sensibilização" e o trabalho de especialização efetuado no NCiber (17%) (quadro 5). Em relação às dificuldades, é apontado em 33% que o policiamento no ciberespaço é muito diferente do tradicional, principalmente no que toca ao policiamento preventivo e à visibilidade policial (quadro 5) e a incapacidade da PSP realizar esta monitorização, como já notado supra, a nível de recursos humanos e logísticos, por 17%.

Quanto à quarta questão: Na sua perspetiva, existem particularidades a ter em conta no "patrulhamento" do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal? - Na subcategoria "especificidades de enquadramento de espaço" (quadro 8), 83% referem que não se "patrulha" o ciberespaço da mesma forma que no espaço físico: "Não podemos patrulhar o ciberespaço da mesma forma como patrulhamos uma cidade" (informador 1, mestre em cibercrime, quadro 7), 50% aludem à necessidade de adaptação das ferramentas e métodos ao ciberespaço, "*expertise* específica" e a criação de uma estrutura eficaz (quadro 7). Este espaço é caracterizado por 17% dos entrevistados, como virtual e ausente de fronteiras, possuindo ainda especificidades quanto à disponibilidade, a integridade e a confidencialidade da informação (17%), onde as pessoas têm a capacidade de se anonimizar e mascarar a sua identidade (17%) e permite o aperfeiçoamento técnico das ferramentas utilizadas pelos cibercriminosos, tornando-as diferentes da de um criminoso tradicional (17%) (quadro 8).

Analisando a questão cinco: Quanto controlo *online* é necessário e quando é demasiado? – Relativamente à necessidade (quadro 10), 33% declaram de forma positiva a sua existência, uma vez que é premente que se consiga chegar à identificação de quem comete crimes *online* (33%), defendendo a Chefe do NCiber (Inf 2) que este controlo, por parte das autoridades, "não é um controlo propriamente dito" e que "não é necessário andarmos a controlar o que a pessoas fazem na *internet*, temos é de ter a capacidade de conseguir identificar as pessoas que cometem crimes" (quadro 9). A identificação da obrigatoriedade de existir mecanismos legais para as operadoras é referida por 17% assim como a existência de controlo parental. Ainda na subcategoria necessidade, o especialista em cibersegurança (Inf 4), acredita que o controlo só faz sentido numa ótica de sinalizar condutas ilegais e atuar somente sobre essas (quadro 9). Em oposição, o Chefe do NAOP (Inf 5), defende a criação de equipas direcionadas apenas a esta atividade. Do outro lado da

questão, os "limites", observa-se que 67% apontam o equilíbrio que tem de ocorrer entre os deveres de investigação e os Direitos Fundamentais das pessoas, sendo que 17% mencionam as liberdades das pessoas e os outros 17% a proporcionalidade e a adequação dos meios.

No que tange à sexta questão: Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos? – Obtiveram-se 14 ideias distintas por parte dos 6 informadores, conforme mostra o quadro 2.

Quadro 2- Categorização da questão n.º6 "Em relação ao MIIP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?"

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
MIPP	Valências	6.1.Escola Segura	X			X	X		3	50%
		6.2. Sensibilização da população idosa	X				X		1	33,3%
		6.4. Todos os recursos no quadro do MIPP		X				X	2	33,3%
		6.5. Sensibilização dos pais		X		X			1	33,3%
		6.6. Educação dos professores		X					1	16,7%
		6.7. Dissuasão dos potenciais criminosos		X					1	16,7%
		6.10. Ações de sensibilização em grande número nas escolas				X			1	16,7%
		6.11. Aula lecionada por um polícia				X			1	16,7%
		6.12. Publicações nas redes sociais					X		1	16,7%
	Limitações e obstáculos	6.3. Ações insuficientes e pouco abrangentes	X	X	X		X		4	66,7%
		6.8. O trabalho do MIPP não é suficiente			X				1	16,7%
		6.9. A estrutura deve estar na repressão			X				1	16,7%
		6.13. RH devidamente formados						X	1	16,7%
		6.14. Necessidade de validação dos conteúdos formativos						X	1	16,7%

Na subcategoria "valências", 50% dizem que a Escola Segura é quem mais contribui e 33% fazem referência a todos os recursos afetos ao MIPP em geral. Como contribuem? 33% indicam com ações de sensibilização à população idosa, 33% sensibilizando os pais e 17% apostando na educação dos professores. Ademais salienta-se o papel na dissuasão de potenciais criminosos (17%) e as frequentes publicações nas redes sociais (17%). O Inf 4 ainda recomenda a introdução de uma componente letiva, à semelhança do que acontece na Holanda, ministrada por um polícia, no currículo académico dos alunos, pois seria uma mais-valia a três níveis: "trabalhar a imagem da Polícia, a relação com os jovens e desconstruir a imagem da Polícia, sobretudo junto dos jovens que têm uma imagem mais negativa" (quadro 11). A limitação mais notada, por 67%, é o facto de as ações de sensibilização/formação serem ainda escassas e pouco abrangentes, devendo o MIPP atuar junto de toda a população e identificar outros grupos vulneráveis (quadro 11). No entanto, 17% defendem que já se realizam ações em grande número nas escolas (6.10.). Para além disso, os informadores sinalizam a fraca formação do efetivo do MIPP (17%) e a necessidade de validação, por entidades externas, dos conteúdos formativos (17%). Por último, o chefe do NAOP, convictamente, salienta que o caminho não passa pelo trabalho do MIPP, "não é suficiente" e "o principal é nós termos uma estrutura de investigação criminal célere e eficaz; a estrutura deve estar na repressão" (quadro 11).

Em análise à sétima questão: Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique. – Quanto ao público-alvo, 50% dos informadores destacam que se deve começar pelas crianças e os jovens, sendo que 33% salientam também os idosos. De outra forma, 17% indicam que se deve atuar em todo o público-alvo, 17% junto dos pais e ainda 17% eventualmente junto de pessoas que têm problemas de adição ao jogo, problemas de impulsividade em compras *online* ou em partilha de conteúdos prejudiciais para si próprias, entre outros grupos que sejam identificados. Justificando o porquê da prevalência das crianças, 67% salientam a sua ingenuidade, a exposição contínua às TIC e porque são o futuro e os próximos decisores (quadro 13). No que respeita aos idosos, 17% afirmam a necessidade de investimento nesta população pois são tanto ou mais vulneráveis que os mais jovens, assim como 17% abordam o envelhecimento da população, a grande percentagem de infoexcluídos e a questão da solidão e dos fatores psico-motores (quadro 13). Em toda a população, visto cada tipologia criminal estar mais associada a um determinado público-alvo (17%) (quadro 14).

A despeito da oitava pergunta: Quais os riscos que correm as crianças ao navegar na *internet*? – Foram definidas quatro subcategorias. Nos riscos de "ordem psíquica", 17% referem a sujeição a conteúdos inadequados para a idade, como o *phishing*, burlas ou *cyberbullying* (quadro 15) e 17% a perda de faculdades de inter-relacionamento e problemas de controlo comportamental. Nos riscos de "ordem criminal", são mencionados dois: os crimes sexuais, por 50% dos entrevistados, apesar de o Chefe do NAOP, considerar não ser preocupante aqui em Portugal (quadro 15, unidade de registo 8.7) e 17% o perigo de serem vítimas de extorsão. O risco de fazerem *download* de programas que contenham *malware* ou reservados a direitos de autor e a falta de controlo existente na disseminação de conteúdos que possam ser perniciosos para a sua saúde, ambos relatados por 17%, correspondem à subcategoria "de ordem tecnológica". Na última subcategoria "de ordem material", 50% notaram a falta de consciência das crianças para os riscos que correm ao navegar na *internet* e 17% salientaram as questões relacionadas com a própria privacidade. O Inf 4 afirma ainda que os riscos que as crianças correm ao navegar na *internet* são os mesmos que correm no mundo físico, com a ligeira diferença de que no segundo é mais fácil sinalizar a ameaça (quadro 15, unidade de registo 8.8). Por último, a ideia de que o elencar destes perigos deve ser uma missão da PSP para poder priorizar os conteúdos formativos, é defendida pelo Oficial de Ligação da PSP (Inf 6) (quadro 15, unidade de registo 8.12).

Analisando a nona e última pergunta: Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar? – No que toca aos desafios, 50% afirmam que já existem atualmente e são eles: a velocidade da informação, referida por 50%; a interconectividade dos sistemas, a evolução do *modus operandi* dos cibercriminosos e as ameaças, particularmente quanto à vertente da segurança interna, cada uma indicada por 33%; as *fake news*, os algoritmos (inteligência artificial) e a inexistência em Portugal e consequentemente na Polícia de uma cultura de defesa a nível da cibercriminalidade (17%). Quanto à forma de os ultrapassar, 33% apontam a formação dos recursos humanos, 17% a criação de uma estrutura eficaz, 17% fazem referência à existência de ciberpoliciamento, 17% assinalam o aumento da resiliência digital da população, 17% salientam a importância da preocupação com a Pessoa e não com o grupo de pessoas, para se poder direcionar eficazmente as prioridades de prevenção (quadro 17) e, por fim, destaca-se o recrutamento de peritos externos, por 17% dos entrevistados (quadro 18).

4.3.2. Análise estatística ao Questionário[6]

Neste subcapítulo analisar-se-ão as variáveis sociodemográficas relativas aos educandos e aos EE. Esta análise é complementada com os dados resultantes dos cruzamentos entre as variáveis selecionadas.

No que se refere às crianças, em particular à variável "idade" (quadro 19 e gráfico 1), constata-se que 30% têm sete anos de idade, 21% nove anos de idade, 21% oito anos de idade, com seis anos de idade 16% das crianças, com dez anos 9% e onze e doze anos apenas 1% e 0,4% das crianças, respetivamente. As idades são compreendidas entre seis (mínimo) e doze (máximo). Na variável "sexo" (quadro 20 e gráfico 2) ou identidade de género, obteve-se cerca de 50% do sexo feminino e cerca de 50% do sexo masculino. Observa-se a maior percentagem de crianças no 2º "ano de escolaridade", com cerca de 33%, de seguida no 4º ano, com cerca de 26%, no 1º ano com 23% e por fim 18% das crianças no 3º ano (quadro 21 e gráfico 3). Respeitando às "habilitações literárias" dos EE (quadro 22 e gráfico 4), é possível verificar que mais de metade não possui o Ensino Superior (64%), contando com 29% os que possuem Licenciatura, 6% Mestrado e 1% Doutoramento.

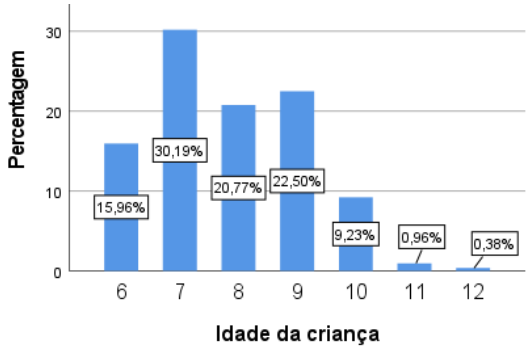


Gráfico 1- Idade da criança

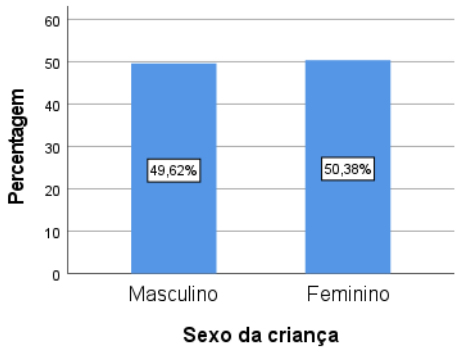


Gráfico 2- Sexo da criança

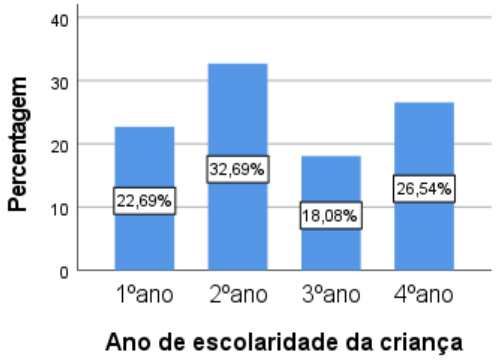


Gráfico 3- Ano de escolaridade da criança

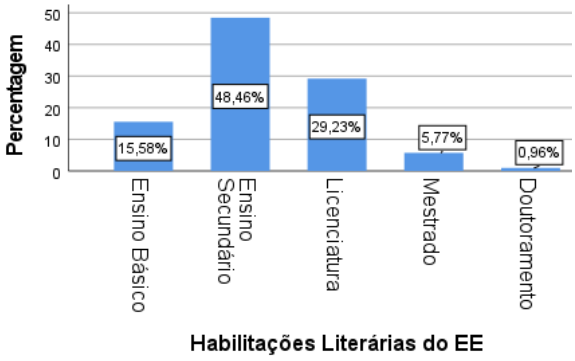


Gráfico 4- Habilitações literárias dos EE

[6] Os quadros referentes à análise estatística dos resultados do questionário encontram-se no Apêndice J.

A nível da "frequência nos dispositivos digitais" é de notar que cerca de 32% das crianças acedem à *internet*, diariamente ou quase, no seu telemóvel pessoal, enquanto nos outros dispositivos a maior percentagem corresponde à opção "nunca", observando-se ainda 12% no computador diariamente e 18% no *tablet* (quadro 23). A "consola", referida de forma residual, deriva da codificação da categoria "outro", tendo sido a única ocorrência registada. O *smartphone* é a tecnologia digital mais utilizada, sendo as crianças dos oito aos doze anos de idade (quadro 43) e as raparigas (gráfico 5) que mais o utilizam. O computador, o *tablet* e a consola são mais utilizados pelos rapazes (gráficos 6, 7 e 8) e também por quem se situa nos oito aos doze anos (quadros 45, 47 e 49). No que se refere à relação entre as variáveis, mesmo tendo recodificado, criando apenas dois escalões de idade, verificou-se que, em todos os cruzamentos efetuados entre esta variável e as restantes consideradas hipoteticamente dependentes, não se verificou haver uma relação estatisticamente significativa entre as variáveis. Ou seja, não se rejeita a hipótese nula e rejeita-se a hipótese alternativa em todos os cruzamentos com a variável idade recodificada (quadros 44, 46, 48 e 50).

Assinala-se que "o tempo que as crianças em estudo passam sozinhas na *internet* num dia de semana e num dia no fim de semana" é residual (quadros 24 e 25). Em ambos os casos, a maior percentagem equivale à opção "pouco tempo ou nenhum", com cerca de 42% e 23%, respetivamente. Cerca de uma hora, num dia de semana, corresponde a aproximadamente 25%, enquanto num dia de fim de semana, duas horas foram referidas por cerca de 22% dos EE. Com base nos quadros 51 e 52, refira-se que cerca de 4% das crianças estão cinco horas, cerca de 2% estão seis horas, cerca de 1% estão sete e até oito horas (1%), num dia do fim de semana, na *internet* (quadro 52). Cinco EE não sabem quanto tempo os seus educandos passam na *internet* sozinhos num dia de fim de semana (quadro 52). As crianças no escalão etário dos oito aos doze anos passam sensivelmente mais horas na *internet* do que as crianças mais novas.

Nos seus tempos livres, a maior parte das crianças "faz os trabalhos ou outras atividades escolares" (80%), "ajuda nas tarefas domésticas" (59%), "faz atividades ao ar livre" (58%) e "pratica desporto ou outras atividades físicas" (53%) (quadro 26). Apenas cerca de 17% "conversa e diverte-se com amigos *online*", os quais abrangem maioritariamente (90%) as idades dos oito aos doze anos (quadro 53), enquanto pessoalmente equivale a cerca de 40% (quadro 26). O convívio *online* é repartido pelos rapazes e raparigas (50%), assim como fisicamente (cerca de 50%) (quadros 54 e 55). Praticar atividades desportivas, jogar videojogos e fazer atividades ao ar livre são mais

associadas aos rapazes (quadros 56, 57 e 58), enquanto ajudar nas tarefas domésticas ou fazer trabalhos escolares (quadros 59 e 60) às raparigas.

O quadro 3 cruza a frequência com que a criança pratica estas atividades nos tempos livres e as habilitações literárias dos EE, recodificadas em três categorias, em vez de cinco.

Quadro 3- Frequência com que a criança pratica estas atividades nos tempos livres, por habilitações dos EE

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Atividades mais praticadas pela criança nos tempos livres[a]	Pratica desporto ou outras atividades físicas	Frequência	26	116	131	273
		% em $Q3	9,5%	42,5%	48,0%	
		% em Hab_2	34,7%	48,9%	70,8%	
	Joga videojogos	Frequência	27	94	77	198
		% em $Q3	13,6%	47,5%	38,9%	
		% em Hab_2	36,0%	39,7%	41,6%	
	Conversa e diverte-se com amigos *online*	Frequência	12	47	31	90
		% em $Q3	13,3%	52,2%	34,4%	
		% em Hab_2	16,0%	19,8%	16,8%	
	Faz atividades ao ar livre	Frequência	37	132	132	301
		% em $Q3	12,3%	43,9%	43,9%	
		% em Hab_2	49,3%	55,7%	71,4%	
	Conversa e diverte-se com amigos cara a cara	Frequência	22	101	81	204
		% em $Q3	10,8%	49,5%	39,7%	
		% em Hab_2	29,3%	42,6%	43,8%	
	Ajuda a família nas tarefas domésticas	Frequência	43	148	112	303
		% em $Q3	14,2%	48,8%	37,0%	
		% em Hab_2	57,3%	62,4%	60,5%	
Total		Frequência	75	237	185	497
Percentagens e totais têm respondentes como base.						
a. Grupo de dicotomia tabulado no valor 1.						

Neste quadro é possível observar que os educandos de EE com o ensino secundário fazem uma prática mais assídua destas atividades, exceto praticar desporto ou outras atividades físicas que é mais priorizado por quem possui o ensino superior.

No que toca às "alterações comportamentais da criança após a exposição às TIC", constata-se a sua não observância, salvo a opção "fica aborrecida por não poder estar nos dispositivos" que é referida por cerca de 86% dos EE (quadro 28). Ainda nesta variável, pelo exposto no quadro 61, identifica-se que a idade em que mais crianças têm este comportamento é aos sete anos, com cerca de 34%, seguindo-se os oito e os nove (22%).

Nas "situações de risco", responderam de forma positiva somente 42 EE, salientando-se a opção "o dispositivo que a criança usa apanhou um vírus" (37%), "excluíram-na de um grupo na *internet*" (27%), "recebeu mensagens desagradáveis" (17%) e "teve de fazer coisas que não queria" (17%) (quadro 31). 53 EE desconhecem se estas situações já ocorreram com a criança (quadro 32). Em resposta a estas ocorrências, por 25% das vezes os EE "falaram diretamente com os envolvidos" e 75% "não fizeram nada" (quadro 33). A pergunta n.º 7 relativa à resposta das autoridades não se aplica, porquanto não obteve respostas.

Na questão 8 "Cuidados instaurados pelos EE no acesso da criança à *internet*", a opção com maior percentagem é "vigio, não a deixando sozinha", com mais de metade respostas afirmativas (69%) (quadro 35). O cuidado que os EE menos adotam é "instalei um *software* de registo de histórico da *internet*, com apenas 11%. Com base no quadro 55, regista-se que dos 54 EE que instalaram um "*software* de registo de histórico da *internet"*, cerca de 93% possui o Ensino Secundário e Superior e com o Ensino Básico, somente cerca de 7% tem este cuidado. O mesmo acontece nas restantes opções, por exemplo, quem mais "vigia, não deixando a criança sozinha" são os EE que têm o Ensino Secundário. Em suma, quem possui apenas o Ensino Básico, tem prevalência por vigiar e/ ou sensibilizar, ao passo que quem tem mais qualificações prioriza as opções "configurei um bloqueio das horas de acesso" e "coloquei um filtro *web*". Ainda em relação a esta variável, relacionando com a idade da criança (quadro 63), é possível observar a maior preocupação dos EE na adoção de cuidados mais técnicos quando os seus educandos são mais velhos (8-12 anos) e vigiar, não deixando a criança sozinha quando aqueles têm seis e sete anos. Contudo, existe uma grande percentagem de EE com o ensino superior que apenas sensibiliza no que toca ao escalão etário mais elevado (73%).

Em relação às "práticas de mediação entre crianças e tecnologias por parte dos pais", como assim lhes chamam Ponte et al. (2020, p.34), conclui-se que, de uma forma geral, os EE apostam moderadamente nestas ações: encorajar a criança a explorar e aprender coisas na *internet* (37%), sugerir modos de usar a *internet* de forma segura (33%), falar com a criança sobre o que ela faz *online* (38%) e ajudar a criança quando algo a aborrece na *internet* (33%) (quadro 37). No sentido de perceber se estas variáveis se relacionam com a variável "habilitações literárias" foi elaborado inicialmente o quadro 64, constatando-se que não rejeitamos a hipótese nula e rejeitamos a hipótese alternativa, ou seja, estas duas variáveis não são dependentes entre si (quadro 65).

Quadro 4- Frequência com que o EE encoraja a criança a explorar na *internet*, por habilitação literária

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Encoraja-a a explorar e a aprender coisas na *internet*	Nunca	F	17	38	20	75
		% em Encoraja-a	22,7%	50,7%	26,7%	100,0%
		% em Habilitações	22,1%	16,7%	11,4%	15,6%
	Quase nunca	F	5	30	23	58
		% em Encoraja-a	8,6%	51,7%	39,7%	100,0%
		% em Habilitações	6,5%	13,2%	13,1%	12,1%
	Algumas vezes	F	36	90	66	192
		% em Encoraja-a	18,8%	46,9%	34,4%	100,0%
		% em Habilitações	46,8%	39,5%	37,5%	39,9%
	Muitas vezes	F	12	50	42	104
		% em Encoraja-a	11,5%	48,1%	40,4%	100,0%
		% em Habilitações	15,6%	21,9%	23,9%	21,6%
	Quase sempre	F	7	20	25	52
		% em Encoraja-a	13,5%	38,5%	48,1%	100,0%
		% em Habilitações	9,1%	8,8%	14,2%	10,8%
Total		F	77	228	176	481
		% em Encoraja-a	16,0%	47,4%	36,6%	100,0%
		% em Habilitações	100,0%	100,0%	100,0%	100,0%

Quadro 5- Teste qui-quadrado das variáveis frequência com que o EE encoraja a criança a explorar na *internet* e habilitações literárias

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	12,469[a]	8	,131
Razão de verossimilhança	12,819	8	,118
Associação Linear por Linear	5,433	1	,020
N de Casos Válidos	481		
a. 0 células (0,0%) esperavam uma frequência menor que 5. A frequência mínima esperada é 8,32.			

Deste modo, foram novamente reconfigurados os três graus académicos Licenciatura, Mestrado e Doutoramento na variável "ensino superior". Não obstante, continuou-se a obter os mesmos resultados, como se visualiza nos quadros 4 e 5 supra e até ao quadro 71 em apêndice.

No que tange à escola, surge a questão 10, mostrando que, em ambas as escolas, nos últimos 12 meses, a proporção de idas da Escola Segura foi de 51%, cerca de 20% das crianças têm aulas que as ensinam a lidar com os benefícios e riscos da *internet* e cerca de 37% fruem de aulas em que são consolidadas as competências digitais (26%) (quadro 38). Não se observa relevante preocupação na obtenção de informação sobre cibereducação, por

parte dos EE (36%). Em concreto, relacionando com o ano de escolaridade, notou-se a presença da Escola Segura maioritariamente no 4.º ano e ambas as aulas igualmente no 4.º ano (gráficos 9, 10 e 11). O quadro 72 expõe a proporção das idas da Escola Segura, com cerca de 40% na Escola Básica José Tagarro e cerca de 60% na Escola Básica Manuel Coco. Ainda nesse quadro, assinala-se alguma diferença, quanto ao leccionamento de aulas onde sejam ministradas competências digitais, com a escola no Cartaxo a possuir uma percentagem muito superior, 77%, contra 23% na escola em Odivelas. Nesta conformidade, as medidas a que os EE dão maior importância (quadro 40) são: "maior investimento nas idas da Escola Segura à escola" (cerca de 90%), "maior proximidade da Polícia com a comunidade escolar" (cerca de 37%) e "maior investimento na formação dos pais" (cerca de 37%). Acrescem outras 8 medidas identificadas pelos EE na resposta à pergunta "Outra. Qual?", destacando-se: a criação de uma aplicação a nível nacional para as escolas com conteúdos e entretenimento, a escola dever bloquear todos os *sites* que não sejam para a formação do aluno a nível escolar e a criação de uma disciplina no programa educativo acerca dos benefícios, riscos e perigos da *internet* (quadro 42).

Comparando as escolas, salienta-se que do universo dos EE, a Escola do Cartaxo apresenta uma proporção mais elevada no que toca ao ensino secundário (cerca de 49%) e superior (cerca de 36%) e a percentagem respeitante ao ensino básico é por sua vez, superior na Escola de Odivelas com cerca de 17% (quadro 73). Os EE dos alunos da Escola no Cartaxo são os que dão maior importância à implementação destas medidas na respetiva escola (quadro 74). Concretamente, a medida mais selecionada por eles é "maior investimento na formação sobre a utilização da *internet* junto dos pais", com 58%. A respeito das atividades nos tempos livres (quadro 75), efetuando a mesma comparação, conclui-se de igual forma: os EE na escola do Cartaxo primam mais pela prática daquelas pelos seus educandos, do que em Odivelas. Com a exceção da atividade "conversa e diverte-se com amigos *online*", em que 60% corresponde às respostas dos EE na Escola em Odivelas, em oposição aos 40% na escola no Cartaxo.

4.4. Discussão de resultados

A revisão da literatura possibilitou alcançar-se os seguintes objetivos: descrever os conceitos em estudo, examinar a evolução do fenómeno da cibercriminalidade no contexto ocidental, caracterizar o ciberespaço, os ofensores e as vítimas, analisar o trabalho do MIPP face ao ciberespaço, examinar o impacto da cibervitimação nas crianças e jovens e identificar as vertentes de atuação da PSP na prevenção destes crimes. Seguidamente, com vista a

atingir os restantes desideratos – conhecer o grau de conhecimento de EE de crianças do 1.º ciclo em relação aos riscos que elas correm com a utilização das TIC e perceber o papel da PSP na prevenção e no combate do cibercrime e aferir a existência de ciberpoliciamento – realizou-se o trabalho empírico apresentado no subcapítulo anterior (entrevistas e inquérito). Assim, os dados recolhidos devem ser verificados quanto à validade e veracidade.

Os resultados decorrentes das entrevistas levantam algumas reflexões. O primeiro objetivo da realização das entrevistas consistia em perceber o papel da PSP na prevenção do cibercrime, identificado como o objetivo geral, mas também até que ponto atua na vertente do combate ao cibercrime, tendo em conta que na literatura pouco se encontrou acerca de ciberpoliciamento em Portugal. A este nível apontam-se os estudos de Maia (2019) acerca do ciberpoliciamento das redes sociais e de Ramos (2022) "O Agente Encoberto Digital". Dos resultados, inferimos a atuação primária da PSP na prevenção do cibercrime. Esta primeira ideia é corroborada com tudo o que foi exposto nesta investigação – as várias vertentes de intervenção, a sensibilização, a formação, a colaboração, a cooperação; a ação do policiamento de proximidade, máxime das EPES e EPAV afetas ao MIPP; a pertinência em trabalhar junto das crianças devido ao impacto da cibervitimação nas suas vidas – e, ainda com várias contribuições dos informadores qualificados, das quais se destaca: "A PSP tem tido um papel ativo nas redes sociais e meios de comunicação social alertando a população para os riscos existentes na utilização das novas tecnologias e da *internet*."; "Desde o início percebemos que a principal forma de se prevenir a cibercriminalidade e combatê-la é o esclarecimento e consciencialização da população para a utilização segura da *internet*, porque é muito difícil chegar aos autores dos crimes por constrangimentos diversos e legais e "Nós, PSP, em concreto na área da prevenção, trabalhamos sempre junto do público mais jovem (…). Para além disso, e porque está também identificado como um público particularmente vulnerável, estamos a trabalhar os idosos, alertando-os também para os cuidados que têm de ter no manuseamento dos dispositivos quando estão na *internet* (…)." Noutros estudos, também esta ideia é apoiada, Poiares (2019, p. 119) afirma: "A começar nas famílias, nas escolas e numa comunicação social responsável rumo a uma higienização digital, sem olvidar o papel insubstituível da PSP e da GNR no domínio da prevenção, área de atuação privilegiada no âmbito da cibersegurança, em detrimento da investigação criminal". Robalo (2021, p.51) defende a importância de "apetrechar os cibernautas de informação e escudos de proteção", enquanto Venâncio (2021, p.95) afirma que a educação para a segurança digital é o "calcanhar de Aquiles" da Cibersegurança.

No que toca ao combate, as opiniões divergem, por um lado defende-se uma intervenção secundária da PSP e de outro, a sua contribuição significativa, inferindo-se também a ideia de que a PSP não tem capacidade para atuar ao nível da investigação destes crimes. De notar, antes de mais, que o domínio de atuação da PSP são os crimes ciber-instrumentais, isto é, aqueles que recorrem aos meios informáticos para serem consumados, pelo que o bem jurídico em causa não será um bem informático, contrariamente aos crimes ciber-dependentes, em que as TIC são o "alvo do crime", a denominada "criminalidade informática" (Verdelho et al., 2003, p. 28) estrita. Apesar destes últimos não estarem no âmbito de ação da PSP, quando se tem conhecimento deles, remete-se a informação ao Ministério Público e ao Órgão de Polícia Criminal competente para a sua investigação. Com o intuito de aprofundar o trabalho nesta área, foi criado o Núcleo de Cibercriminalidade, cuja atividade se insere em ambas as vertentes: apoio à IC – extração e análise de cabeçalhos técnicos (*e-mails* de *phishing*, ameaças, difamação e injúrias por *e-mail* ou outros ilícitos com recurso a *e-mail)*; falsos SMS "Smishing"; burlas; furtos de identidade (redes sociais); participação em operações/ buscas para recolha de dados (preservação da prova digital) -, formação do efetivo, a monitorização em fontes abertas e a difusão de alertas operacionais e no futuro, a aposta será na especialização por áreas, segundo informação fornecida, a título informal à autora, pela Chefe do Núcleo. Em reforço do descrito, refere-se o papel da PSP na identificação de situações que configurem crimes ou outro tipo de atividades que, de certa forma, possam parecer atos preparatórios da prática de crimes e ainda a atuação no campo da violência doméstica, mencionados pelos informadores qualificados.

Nunes (2021) identifica vários entraves da própria *internet* na investigação e prevenção do cibercrime, como a quantidade instrumental de dados e a sua rápida difusão, a interação de um grande número de pessoas, a imaterialidade, a utilização de camadas mais profundas, o contacto remoto entre os intervenientes, o facto de o mesmo IP poder ser utilizado por inúmeros utilizadores e as medidas antiforenses (*passwords* complexas, encriptação das mensagens, criptomoedas, *dark web*, entre outras mais técnicas). No sentido de ultrapassar estes desafios, é primordial a especialização dos polícias e dos meios técnicos ao seu dispor, inclusive repensar o recrutamento de peritos externos e é necessário haver cooperação interna, com as operadoras de comunicações e com o mundo académico e científico, conforme identificado pelos entrevistados. Nesta sede, estão também os autores Santos et al. (2008) e Nunes (2021), acrescentando ainda a cooperação a nível internacional, uma vez que a cibercriminalidade é transnacional, envolvendo maioritariamente servidores localizados fora do país.

O segundo objetivo era analisar a possibilidade de "patrulhar" o ciberespaço e como é/poderá ser feito. Como tal, seria premente perceber se realmente a PSP efetua "ciberpoliciamento", constatando-se de que é realizado um trabalho de monitorização do ciberespaço, quer no Núcleo de Cibercriminalidade, em especial nas redes sociais e em alguns fóruns, quer no Núcleo de Análise do Departamento de IC e ainda no Departamento de Informações Policiais (com base em informação fornecida, a título informal, à autora). No DIP realizam monitorização do ciberespaço, mas no que toca à sua área, nomeadamente manifestações, terrorismo, etc. No Núcleo de Análise faz-se a monitorização de fenómenos com grande impacto a nível nacional, sendo efetuado o seu acompanhamento diariamente (tipo de *modus operandi*, perfil dos suspeitos, características semelhantes, etc.). Em síntese, os analistas leem e analisam todo o expediente feito no Sistema Estratégico de Informação, retiram os dados relevantes e elaboram o estudo da tipologia criminal, difundindo Relatórios Operacionais, que, apoiarão a tomada de decisão dos comandantes no terreno, direcionando o policiamento. Contudo, este Núcleo não faz investigação, nem monitoriza as redes sociais ou pesquisa suspeitos, esse trabalho pertence atualmente ao Núcleo de Cibercriminalidade, assim como o referido supra. Outra atividade que o NCiber tem a seu cargo é a difusão de estratégias de prevenção, sensibilizando a população, os chamados "alertas operacionais". A monitorização realizada nesta valência é direcionada para alvos ou fenómenos específicos (quando o crime já ocorreu e o inquérito foi distribuído à PSP) numa vertente repressiva ou numa perspetiva preventiva, quando há notícia de que vai acontecer um determinado fenómeno criminal.

Por último, verificar a possibilidade de adaptar o policiamento de proximidade ao ciberespaço e como fazê-lo, representa o terceiro objetivo. Depreende-se dos dados obtidos, à semelhança do que já foi explanado neste trabalho, que a adaptação do MIPP ao ciberespaço tem sido proveitosa, com as duas valências (EPES e EPAV), a realizar um intenso trabalho de sensibilização e formação da população, em especial junto das crianças, jovens e idosos. São levantadas questões que a autora já identificara no início do estudo (capítulo 1): a importância da sensibilização e formação dos pais, a educação dos professores e assistentes operacionais na identificação de possíveis crimes em curso na *internet* ou cujo início ocorre na escola, podendo-se repercutir via *online* e a relevância de se efetuar um trabalho também na parte da dissuasão de potenciais criminosos, atuando como diz Clemente (2010, pp.157 e 159) na "antecipação da prevenção" porque "a previsão é uma prevenção da prevenção" e "antecipar o risco é um imperativo policial". Para além disso, a sugestão de ser criada uma aula no currículo escolar dos alunos, lecionada por um polícia é inteiramente

apoiada e incentivada pela autora deste estudo, porquanto "trabalhava a imagem da Polícia, melhorava a relação com os jovens e ajudava a desconstruir a imagem da Polícia" (Inf 4). Assim como, é imperativo identificar-se outros públicos-alvo, carentes de intervenção por parte do MIPP, na impossibilidade de se apostar em todo o público-alvo, pois "qualquer pessoa pode ser vítima de cibercrime" (Inf 2) e dependendo do tipo de cibercrime, poderão haver fatores de risco para a sua vitimação. A intervenção aqui implica conhecer esses fatores, mas também assegurar o acompanhamento das vítimas e a punição dos agressores (Sani et al., 2018), daí ser fundamental existir uma cultura de denúncia dos crimes e de preservação de prova. A ingenuidade e a não consciência do perigo, somado ao elevado tempo despendido na *internet* e na maioria desprovidas de supervisão parental, aumenta a vulnerabilidade das crianças a possíveis riscos, tais como os sinalizados pelos informadores: a exploração de páginas pouco confiáveis (Vara & Sani, 2021); a dependência *online* que leva à perda de faculdades de inter-relacionamento e problemas de auto controlo, entre outros; predadores sexuais; crime de extorsão; *malware*; questões relacionadas com a privacidade. Além desses, existem outros tantos, englobando também os jovens, os idosos, e naturalmente outros tipos de público-alvo (ciberabuso nas relações de intimidade dos adolescentes; *cyberbullying*; crimes nas redes sociais; *cyberstalking*; "ciberburlas românticas", falsos arrendamentos, burlas informáticas, *phishing*, etc.), sendo que no futuro possivelmente existirão novas tipologias.

Em suma, a PSP tem vindo a capacitar-se na prevenção e no combate ao cibercrime, faltando-lhe percorrer caminho para equivaler à *expertise* já criada em países vizinhos, mormente no que toca a parcerias e colaboração com outras entidades, à criação de equipas especializadas ou à utilização de métodos de IC mais eficazes, contudo mais intrusivos, como a "busca *online*" (Ver Nunes, 2021; Campos, 2021; Ramos, 2022). Esta Polícia realiza um trabalho de monitorização e investigação, em várias das suas valências, houve portanto uma adaptação eficaz do policiamento tradicional ao ciberespaço. As dificuldades encontradas nesse processo são as inerentes ao espaço em si, além das já assinaladas anteriormente, identificamos a sua virtualidade e a ausência de fronteiras, a disponibilidade, integridade e confidencialidade da informação, a capacidade de anonimar e mascarar a identidade e ainda a hipótese de sofisticação dos *modus operandi* dos cibercriminosos. Ora, o policiamento quer preventivo, quer repressivo não ocorrerá da mesma maneira que no espaço físico. Partilha-se da opinião de que não é necessário "andar a controlar o que as pessoas fazem na *internet*, mas ter a capacidade de conseguir identificar quem comete crimes *online"*, sem olvidar o respeito pelos direitos fundamentais do cidadão. O MIPP efetua um

trabalho essencial a nível da cibersegurança e cibereducação da população, podendo ainda se reforçar no tocante aos conteúdos formativos, à abrangência das ações de sensibilização e formação, à criação de uma aula ministrada por um polícia e na relação de confiança que têm com os jovens, para a sua educação, na identificação de práticas delituosas e na dissuasão desses comportamentos. Contudo, pelo exposto, é percetível que a prevenção e o combate ao cibercrime requerem outros meios de intervenção que fazem parte da investigação criminal e que devem ser pensados a curto prazo.

Dos resultados obtidos com a aplicação do inquérito por questionário, há a possibilidade de que os EE não tenham noção da quantidade de tempo que os seus educandos passam na *internet*, pois certamente não estão com eles o dia inteiro e quando estão a supervisão não é total. Como afirma Santo (2015, p.36), na aplicação de questionários, existe a hipótese de os inquiridos responderem "o que consideram ser desejável e não o que corresponde à verdade das suas opiniões, comportamentos ou atitudes". No Estudo EU *Kids Online*, em 2020, 84% das crianças e jovens, em Portugal, faziam uso diário do telemóvel para aceder à *internet* (Ponte et al., 2020). Em oposição, neste estudo, essa percentagem é reduzida aos 32%. À semelhança dos resultados conseguidos no estudo referido, também aqui se constatou que as raparigas ajudam nas tarefas domésticas ou ocupam o tempo com atividades escolares mais do que os rapazes, e estes praticam mais atividades desportivas ou ao ar livre (Ponte et al., 2020). No presente estudo, não se analisaram as diferenças de género em relação às práticas de mediação entre crianças e tecnologias por parte dos EE, pois não revelou interesse, importando apenas notar que podiam ser adotadas mais frequentemente, assim como os cuidados no acesso da criança à *internet*, que se afigurou serem muito pouco privilegiados. Como afirma o Inf 5: "A regulação parental e os instrumentos para essa regulação parental existem e devem ser do conhecimento dos pais e acionados por eles mas isso não dispensa a vigilância que os pais devem prestar, fazer e acompanhar as crianças naquilo que estão a ver".

Foi possível identificar as poucas idas da Escola Segura às duas escolas, nos últimos doze meses, apesar de haver incorreções, pois existem EE de alunos da mesma turma que afirmam positivamente e outros de forma negativa, evidenciando igualmente a pouca conversa existente entre eles e os seus educandos. O mesmo se passa com as aulas. Fica-se sem perceber se os alunos têm aulas nas quais lhes seja ensinado a lidar com os riscos e benefícios da *internet*. As TIC são ministradas em todos os anos de escolaridade obrigatória, com a exceção do 1.º ciclo e do 12.º ano, em que é opcional. No 1.º ciclo as TIC são uma "área de integração curricular transversal" (Ponte et al., 2020, p.60). Ou seja, no 1.º ciclo,

não existe a disciplina de TIC, não obstante, são introduzidos recursos educativos digitais nas outras disciplinas. Aliás, atualmente, os professores são obrigados a fazer uma formação em recursos educativos digitais de dois níveis. Portanto, são apenas consolidadas, de certa forma, as competências digitais, não existindo a vertente dos riscos e da educação cibernética. Não deixa de ser curioso que no Cartaxo a proporção com que o mencionado acontece é muito superior em comparação com Odivelas. Porém a Escola Segura esteve menos presente, daí possivelmente serem os EE que selecionaram mais a medida "maior investimento na formação sobre a utilização da *internet* junto dos pais".

Em síntese, infere-se que o grau de conhecimento dos EE em relação aos perigos que os seus educandos, que frequentam o primeiro ciclo, correm na *internet*, é baixo, não havendo relevante preocupação em adotar cuidados no seu acesso aos dispositivos digitais (poderá relacionar-se com as suas qualificações académicas), nem na sua cibereducação, nem na eventual dependência *online*, visto que a proporção de crianças que ficam aborrecidas aquando do impedimento em utilizar aqueles aparelhos é grande (apesar das horas que passam sozinhas na *internet* não serem tão elevadas, quanto o expectável).

Conclusão

A cibercriminalidade é um conceito polissémico, abrangendo uma panóplia de tipos de ilícitos criminais, pelo que pode levantar questões acerca da competência para a sua investigação por parte das Polícias, por conseguinte, nesta investigação optou-se por se considerar que engloba todo o crime informático e o crime praticado com recurso às TIC.

Se o direito à segurança existe no mundo *offline*, também no ciberespaço ele deve ser garantido, a denominada cibersegurança. As redes sociais, por exemplo, já vão tendo mecanismos de eliminar conteúdo impróprio ou que tenha sido denunciado por muitas pessoas, com a ajuda dos "moderadores de conteúdo", o que também prova que ainda não se consegue apenas com a inteligência artificial. Grande parte do trabalho da Polícia e da PSP, em especial, começa após o cometimento do ilícito ou quando há sinais de que poderá despoletar um determinado fenómeno criminal. A dificuldade em antecipar condutas delituosas é grande, daí a aposta ter de ser a prevenção, enquanto a capacidade de investigação destes crimes for reduzida. As características inerentes ao ciberespaço e à cibercriminalidade, como a transnacionalidade, o anonimato, a a-temporalidade e o impacto dificultam a prevenção destes ilícitos.

O ciberespaço afeta a dinâmica das relações sociais e direitos fundamentais como a liberdade, a segurança e a privacidade. Por um lado, permite a liberdade de expressão, do acesso à informação ou de criação, mas até que ponto? A liberdade de alguém termina quando entra na liberdade de outrem. Existem normas e regras de convivência, o chamado controlo social que é partilhado no mundo físico e no mundo ciber. Ou pelo menos assim devia ocorrer. A realidade é esta: o sentimento de segurança ou a sensação de proteção que se faz sentir na população pela presença da Polícia na rua, não existe neste espaço virtual. Porque mesmo que se "patrulhe" o ciberespaço, os contornos dos policiamentos serão sempre diferentes, o conceito de prevenção não terá o mesmo significado. Por um lado, não só o efeito de desinibição é muito superior, facilitando a prática delitual, como a dissuasão policial é inexistente, não sendo possível efetivar um policiamento de visibilidade. Ademais, também não é possível intervir fisicamente e no imediato aquando do visionamento de um crime. Prevenção neste âmbito tem de ser vista de duas perspetivas: numa ótica de cibereducar e sensibilizar o cidadão e do prisma da investigação, uma vez que a monitorização das fontes abertas também serve para sinalizar e antecipar crimes e os alertas operacionais decorrentes dessa monitorização acerca de fenómenos criminais (perfil e *modus operandi* dos criminosos, como atuam e com quem atuam) permitem não só, igualmente

consciencializar e alertar a população, como auxiliar o policiamento no terreno, pois são difundidos aos OCS e ao efetivo das esquadras, o que também constitui uma forma de prevenção.

O problema de investigação deste estudo remetia para a atuação da PSP no que diz respeito ao cibercrime e à sua prevenção, elencando-se como pergunta de partida: "De que forma a PSP pode contribuir para a cibersegurança e consequentemente prevenir o cibercrime?". Antes de mais, é possível afirmar que esta força de segurança atua nas duas vertentes: a prevenção e o combate. A PJ não detém a exclusiva investigação do cibercrime, pois os crimes ciber-instrumentais cabem à PSP resolver. Em relação ao combate, a PSP ainda está longe da eficácia e especialização que acontece noutros países. Por esse motivo e porque a prevenção é a chave para o combate ao cibercrime, visto que investigar também é prevenir, a perspetiva adotada neste trabalho foi direcionada para a primeira vertente. Respondendo à pergunta de partida, a PSP contribui para a cibersegurança nas suas múltiplas áreas de intervenção, mormente através da sensibilização e da investigação criminal, dado que o fator humano é a peça chave no mundo ciber e, é nele que se deve apostar, a nível dos seus comportamentos e atitudes, em ordem a prevenir o cibercrime.

No que se refere às cinco áreas de intervenção, conclui-se que, é necessário dar formação à totalidade do efetivo da PSP para se conseguir transmitir o conhecimento internamente e auxiliar na IC, mas também externamente, à população, mormente pais, professores, educadores, assistentes operacionais e OCS. A longo prazo, o objetivo será a especialização por áreas, no NCiber.

Na área da sensibilização, cabe ao MIPP, com as suas valências (EPES e EPAV) e programas especiais (*Escola e Universidade Segura, Idosos em Segurança, Comércio Seguro, Internet em Segurança*, etc.) consciencializar toda a população (redes sociais, OCS, palestras, ações de sensibilização e de formação, atividades que promovam o encontro dos cidadãos, atividades no seio escolar, em lares, casas de acolhimento, estabelecimentos comerciais, etc.), maiormente em públicos identificados como vulneráveis e que apresentem vários fatores de risco preditores de vitimação. De referir a consciencialização dos pais de crianças mais novas, porque, como se constatou, existe, da parte deles, pouca preocupação e cuidado no acesso dos filhos à *internet*.

A colaboração com o setor privado, mundo académico e científico, permite à PSP obter a capacidade técnica, logística e o conhecimento necessários para a IC ou na criação de conteúdos educativos, que devem ser revistos e atualizados, conforme a matéria e as faixas etárias em que são ministradas, por exemplo um tópico que não é abordado e devia

ser é a dependência *online* (apesar de estar contemplado estrategicamente). O Centro Nacional de Cibersegurança pode ser um parceiro da PSP pois disponibiliza 4 cursos *e-learning* (cidadão ciberseguro, cidadão ciberinformado, consumidor ciberseguro e cidadão cibersocial) entre outros, e coordena o Consórcio do Centro *Internet* Segura que visa a sensibilização, o esclarecimento, o apoio à população e a denúncia de conteúdo ilegal (CNCS, 2021c), o que consubstancia também a missão desta Polícia. A aposta na formação e a consciencialização do público a nível externo e interno, devem constituir os objetivos da PSP. A colaboração com os OCS, na difusão de informação relevante, para que estes partilhem com o país e ainda a colaboração com as operadoras de comunicação, que possuem dados imprescindíveis à prossecução da investigação, carecendo de protocolos.

Em relação à cooperação internacional, aquando de um cibercrime perpetrado noutro país, a PSP fica dependente da cooperação da sua parte, pelo que o interesse deve ser pugnar para que haja essa interajuda e partilha de informação. Por último, a nível da IC, para além do que já foi referido, a recente unidade especializada criada nesta área, o Núcleo de Cibercriminalidade, será a grande aposta no futuro e o combate ao cibercrime passará em larga escala por aqui.

Em segundo lugar, conclui-se que, na aceção da palavra policiamento, a PSP não realiza ciberpoliciamento. Não existem equipas a "patrulhar" o ciberespaço constantemente. Existe um trabalho de monitorização direcionado ou um acompanhamento a determinadas tipologias de crime (e.g. burlas, roubos, furtos no interior de residência, violência no desporto, *phishing*, *smishing*, etc.), podendo-se identificar condutas que possam parecer atos preparatórios da prática de crimes e ainda chegar aos autores dos crimes. No NCiber, é realizada a monitorização de fontes abertas, quando há essa disponibilidade, a suspeitos já identificados ou a tentativa de ter acesso e obter informação relativa a determinado fenómeno criminal em fóruns de conversação.

As limitações à realização deste estudo respeitam à ausência de colaboração por parte de informadores qualificados na área da psicologia, vitimologia e criminologia e o facto de a dimensão da amostra não ser representativa do universo de EE de crianças a frequentar o 1.º ciclo a nível nacional. Em futuras investigações, recomenda-se a abrangência do estudo, com o contributo de outras áreas das ciências sociais e humanas e de outros países, abordar em profundidade a vertente do combate ao cibercrime, abarcar uma população mais significativa ou mudar de universo e identificar outros públicos-alvo vulneráveis no ciberespaço.

Referências

Alcobia, A., Alturas, B., & Diogo, C. (2020, junho). Tecnologias e População Sénior: Desafios e Oportunidades. [Sessão de Conferência]. ISTAR-CRI- Comunicações a conferências internacionais. https://repositorio.iscte-iul.pt/bitstream/10071/22724/1/conferenceobject_73595.pdf

Alexandrou, A. (2021). *Cybercrime and Information Technology. Theory and Practice-The Computer Network Infrastructure and Cmputer Security, Cybersecurity Laws, Internet of Things (loT), and Mobile Devices.* CRC Press.

Al-Shalan, A. (2006). *Cyber-Crime Fear and Victimization: An Analysis of a National Survey* [Tese de Doutoramento, Faculty of Mississippi State University]. Scholars Junction Mississippi State University Institutional Repository.

Amador, N. (2018). *Cibercrime em Portugal-Trajetórias e Perspetivas de futuro. Pelo Direito a Navegar na Internet em Segurança.* Chiado Editora.

American Psychological Association. (2019). *Digital Guidelines: Promoting Healthy Technology Use For Children*. https://www.apa.org/topics/social-media-*internet*/technology-use-children#

Antunes, M., & Rodrigues, B. (2018). *Introdução à Cibersegurança. A Internet, os Aspetos Legais e a Análise Digital Forense.* FCA-Editora de Informática, Lda.

Arcserve. (2020). *The 2020 Data Attack Surface Report*. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2020/12/ArcserveDataReport2020.pd

Asam, A. E., Samara, M., & Terry P. (2018). Problematic *Internet* Use and Mental Health Among British Children and Adolescentes. *Addictive Behaviors, 90,* 3-32. https://pt.booksc.org/book/72393396/ff61e0

Associação Portuguesa de Apoio à Vítima para jovens. (s.d). *Violência Online: Como se Sente a Vítima?*. Acedido fevereiro 20, 2022, de https://www.apavparajovens.pt/pt/go/como-se-sente-a-vitima6

Associação Portuguesa de Apoio à Vítima. (2019). *Manual ROAR: da Compreensão e Prevenção do Cibercrime ao Apoio e Empoderamento das Vítimas.* https://apav.pt/publiproj/images/publicacoes/ManualProcedimentosROAR-PT.pdf

Associação Portuguesa de Apoio à Vítima. (2020). *Folha Informativa-Burla*. https://apav.pt/apav_v3/images/pdf/FI_Burla_2020.pdf

Azeredo, Z. (2019). *Teoria e Prática em Investigação Qualitativa.* Edições Piaget.

Baker, B. (2006). Beyond the State Police in Urban Uganda and Sierra Leone. *Africa Spectrum, 41*(1), 55-76. https://pt.booksc.org/book/28052582/b9dce6

Bardin, L. (2016). *Análise de Conteúdo.* Grupo Almedina.

Barrinha, A. (2020). Cibersegurança em Tempos de Pandemia. *IDN Brief, 32*, 2.

Beaming United Kingdom. (2020). *Five Years in Cyber Security. Simple Strategies to Boost Business Resilience*. https://www.beaming.co.uk/wp-content/uploads/2020/07/Beaming-Five-Years-in-Cyber-Security-Report-FINAL2.pdf?vgo_ee=0yddXRFk9TSGnEQ4pTh0IKEQRDA3MX%2FpEanpAS%2Bpt3s%3D

Betts, L. R. (2016). *Cyberbullying: Approaches, Consequences and Interventions.* Springer.

Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015). Cyber Dating Abuse: Prevalence, Context, and Relationship with Offline Dating Aggression. *Psychological Reports, 116*(2), 565-585. https://www.researchgate.net/publication/274010571_Cyber_Dating_Abuse_Prevalence_Context_and_Relationship_with_Offline_Dating_Aggression

Bossler, A, M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware

Infection: an Examination of Routine Activities Theory. *International Journal of Cyber Criminology, 3*(1), 400-420.

Brantingham, P. J., & Faust. F. L. (1976). A Conceptual Model of Crime Prevention. *Crime & Delinquency, 22*(3), 284-296. https://pt.booksc.org/book/30806870/299f6b

Bravo, R. (2014). Open Sources in Cybercrime Investigation: Concept and Implications. *Academia.Edu*, 1-5. https://www.academia.edu/7301278/OPEN_SOURCES_IN_CYBERCRIME_INVESTIGATION_concept_and_implications

Burke, S. C., Wallen, M., Vail-Smith, K., & Knox, D. (2011). Using Technology to Control Intimate Partners: An Exploratory Study of College Undergraduates. *Computers in Human Behavior, 27*, 1162-1167. https://www.academia.edu/7556920/Using_technology_to_control_intimate_partners_An_exploratory_study_of_college_undergraduates

Campenhoudt, L. V., Marquet, J., & Quivy, R. (2019). *Manual de Investigação em Ciências Sociais.* Gradiva.

Campos, J. F. S. (2021). *O Malware como Meio de Obtenção da Prova em Processo Penal*. Almedina.

Caridade, S., & Braga, T. (2019). Versão Portuguesa do Cyber Dating Abuse Questionaire (CDAQ) – Questionário sobre Ciberabuso no Namoro (CibAN): Adaptação e propriedades psicométricas. *Análise Psicológica, 1*(37), 93-105. https://www.researchgate.net/publication/331653318_Versao_portuguesa_do_Cyber_Dating_Abuse_Questionaire_CDAQ-Questionario_sobre_Ciberabuso_no_Namoro_CibAN_Adaptacao_e_propriedades_psicometricas

Caridade, S., Sousa, H. F. P., & Dinis, M. A. P. (2020). Cyber and Offline Dating Abuse in a Portuguese Sample: Prevalence and Context of Abuse. *Behavioral Sciences, 10*(152), 1-14. https://doi.org/10.3390/bs10100152

Carvalho, A. R., & Marques, M. R. M. (2017). Cibereducação como Medida Preventiva no Combate ao Cibercrime. *CYBERLAW by CIJIC.* 11-39. https://www.researchgate.net/publication/340849169_Cibereducacao_como_medida_preventiva_no_combate_ao_Cibercrime

Centro *Internet* Segura. (2022). *Violência no Namoro Online - #logoutaoabuso*. https://www.*internet*segura.pt/noticias/violencia-no-namoro-online-logoutaoabuso

Centro Nacional de Cibersegurança. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

Centro Nacional de Cibersegurança. (2020). *Relatório Cibersegurança em Portugal: Riscos & Conflitos.* Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-riscos-conflitos-2020.pdf

Centro Nacional de Cibersegurança. (2021a). *Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021.* Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf

Centro Nacional de Cibersegurança. (2021b). *O que é a Cibersegurança.* CNCS.gov.pt. https://www.cncs.gov.pt/pt/sobre-nos/#oquee

Centro Nacional de Cibersegurança. (2021c). *Centro Internet Segura*. CNCS.gov.pt. https://www.cncs.gov.pt/pt/centro-*internet*-segura/

Centro Nacional de Cibersegurança. (2021d). *Relatório Cibersegurança em Portugal: Sociedade 2021, 3ªEdição*. Observatório de Cibersegurança. https://www.cncs.gov.pt/docs/relatorio-sociedade2021-observ-cncs.pdf

Cepeda, C. S. P. (2012). *Criança e In/Segurança na internet: estudo de caso no 3º Ciclo do*

Ensino Básico [Dissertação de Mestrado, Instituto Politécnico de Beja]. Biblioteca Digital do Instituto Politécnico de Bragança.

Chen, L., Ho, S. S., & Lwin, M. O. (2017). A Meta-analysis of Factors Predicting Cyberbullying Perpetration and Victimization: from the Social Cognitive and Media Effects Approach. *New Media & Society, 19*(8), 1194-1213. https://dr.ntu.edu.sg/handle/10356/142038

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology, 2*(1), 308-333.

Clark, D. (2010). Characterizing Cyberspace: Past, Present and Future. *Office of Naval Research,* 1-18.

Clemente, P. J. L. (2010). Polícia e Segurança: Breves Notas. *Lusíada. Política Internacional e Segurança*, (4), 141-171. http://revistas.lis.ulusiada.pt/index.php/lpis/article/view/146/135

Clevenger, S., Navarro, J. N., Marcum, C. D., & Higgins, G. E. (2018). *Understanding Victimology. An Active-Learning Approach.* Routledge.

Coelho, A. R. (2019). *Seniores 2.0: Inclusão Digital na Sociedade em Rede* [Tese de Doutoramento, Escola de Sociologia e Políticas Públicas]. Repositório Institucional do Instituto Superior de Ciências do Trabalho e da Empresa – Instituto Universitário de Lisboa.

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review, 44*(4), 588-608. https://www.researchgate.net/publication/238322365_Social_Change_and_Crime_Rate_Trends_A_Routine_Activity_Approach

Costa, A. M. L. (2014). *Redes Sociais na Internet: o que Fazem as Crianças/jovens e o que Pensam os Encarregados de Educação* [Dissertação de Mestrado, Universidade do Minho: Instituto de Educação]. Repositório Institucional da Universidade do Minho.

Costa, C. M. S. G. (2007, outubro dezembro). Prevenção da Criminalidade. Idade Viva… *Revista Polícia Portuguesa, 005*(3), 32-34.

Costa, F. A., Viana, J., Cruz, E., & Pereira, C. (2015, novembro). Literacia Digital de Adultos: Contributos para o Desenvolvimento de Dinâmicas de Formação. Simpósio Internacional de Informática Educativa [Simpósio]. Literacia Digital de Adultos, Setúbal. https://www.researchgate.net/publication/289719091_Literacia_Digital_de_Adultos_Contributos_para_o_desenvolvimento_de_dinamicas_de_formacao

Cross, M. (2008). *Scene of the Cybercrime.* (2ªed.). Syngress.

Cunha, A., Gonçalves, M., Martinho, G., & Matos, M. (2021). Ciberespaço e Tráfico De Pessoas: Desafios Atuais para a Criminologia. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 159-180). Pactor.

Cybersecurity and Infrastructure Secure Agency. (2019). *What is Cybersecurity?*. US-CERT.CISA.GOV. https://us-cert.cisa.gov/ncas/tips/ST04-001

Cybersecurity and Infrastructure Security Agency. (2019). *Cyber Safety*. Acedido março 17, 2022, de https://www.cisa.gov/cyber-safety

Daigle, L. E. (2018). *Victimology. The Essentials.* (2ªEd.). Sage Publications, Inc.

Data Reportal. (2021). *Digital Around the World*. Acedido maio 10, 2022, de https://datareportal.com/global-digital-overview

David, M. A. C. (2014). *Modelo Integrado de Policiamento de Proximidade: Funcionalidades, Problemas e Potencialidades* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Científico de Acesso Aberto de Portugal.

Deans, H., & Bhogal, M. S. (2017). Perpetrating Cyber Dating Abuse: A Brief Report on the Role of Aggression, Romantic Jealousy and Gender. *Current Psychology, 38*(5), 1077-1082. http://eprints.staffs.ac.uk/3904/1/Deans%20and%20Bhogal%202017%20-%20Current%20Psychology.pdf

Decreto-Lei n.º 48/1995, de 15 de março. *Diário da República n.º 63/1995- Série I.* Portugal: Ministério da Justiça.

Despacho n.º 6158/2017 de 13 de julho. *Diário da República n.º 134/2017- Série II.* Portugal: Direção Nacional da Polícia de Segurança Pública.

Dhillon, G., & Smith, K. J. (2017). Defining Objectives for Preventing Cyberstalking. *Journal of Business Ethics, 157*, 137-158.

Dias, I. (2012). O Uso das Tecnologias Digitais entre os Seniores: Motivações e Interesses. *Sociologia. Problemas e Práticas*, (68), 51-77.

Dias, P., & Brito. R. (2021). *DIGIKIDS: a Utilização de Tecnologias Touchscreen por Crianças até aos 6 Anos*. https://repositorio.ucp.pt/bitstream/10400.14/32450/3/9789895471942.pdf

Direção Nacional. (2020). Estratégia PSP 20|22. https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Documentos%20Estrat%C3%A9gicos/Estrat%C3%A9gia%20PSP%202020_2022.pdf

Diretiva Estratégica n.º 10/2006, de 15 de maio. Direção Nacional da PSP.

Diretiva Estratégica n.º 3/2022, de 10 de janeiro. Direção Nacional da PSP.

Diretiva Estratégica n.º 43/2021, de 22 de setembro. Direção Nacional da PSP.

Diretiva Estratégica n.º 5/2022, de 24 de janeiro. Direção Nacional da PSP.

Diretiva Estratégica n.º 55/2021, de 11 de novembro. Direção Nacional da PSP.

Dooley, J. J., Pyzalski, J., & Cross, D. (2009). Cyberbullying Versus Face-to-Face Bullying: A Theoretical and Conceptual Review. *Journal of Psychology, 217*(4), 182-188. https://pt.booksc.org/book/71541972/02ba9f

Ekblom, P. (2005). How to Police the Future: Scanning for Scientific and Technological Innovations which Generate Potential Threats and Opportunities in Crime, Policing and Crime Reduction. In Smith, M., & Tilley, N. (Eds.), *Crime Science: New Approaches to Preventing and Detecting Crime*. (pp.27-55). Willan Publishing.

Elias, L. (2009). A (Nova) Governança da Segurança numa Contemporaneidade Complexa. In Manuel, M. G. V. (Coord.), *Estudos Comemorativos dos 25 anos do ISCPSI em Homenagem ao Superintendente-Chefe Afonso de Almeida.* Almedina.

Elias, L. (2018). *Ciências Policiais e Segurança Interna. Desafios e Prospetiva*. Instituto Superior de Ciências Policiais e Segurança Interna.

Elias, L. (2019). Ciberameaças e (In)segurança. *CYBERLAW by CIJIC,* (7), 13-45. https://www.cijic.org/wp-content/uploads/2019/05/Luis-Elias_CIBERAMEA%C3%87AS-E-INSEGURAN%C3%87A.pdf

Elias, L. M. A. (2007). Policiamento de Proximidade – Princípios e Fundamentos para a Implementação de Estratégias de Prevenção Criminal. In *Estudos de Homenagem ao Juiz Conselheiro António da Costa Neves Ribeiro*. (pp. 465-536). Almedina.

European Union Agency for Cybersecurity. (2018). *ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Englander, E. K. (2020). *25 Myths about Bullying and Cyberbullying.* Wiley Blackwell.

EUROPOL. (2020a). *Internet Organised Crime Threat Assessment*. https://www.europol.europa.eu/activities-services/main-reports/*internet*-organised-crime-threat-assessment-iocta-2020

EUROPOL. (2020b, março 27). *Pandemic Profiteering How Criminals Exploit the COVID-*

19 Crisis. https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

EUROPOL. (2020c, novembro 12). *How COVID-19-related Crime Infected Europe During 2020*. https://www.europol.europa.eu/publications-documents/how-covid-19-related-crime-infected-europe-during-2020

EUROPOL. (2020d, junho 19). *Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse During the COVID-19 Pandemic*. https://www.europol.europa.eu/sites/default/files/documents/europol_covid_report-cse_jun2020v.3_0.pdf

Fernandes, L. F. (2006). A Prevenção da Criminalidade. In Valente, M. M. G. (Coord.), *II Colóquio de Segurança Interna. Instituto Superior de Ciências Policiais e Segurança Interna.* (pp.69-114). Almedina.

Fisher, B. S., & Lab, S. P. (2010). *Encyclopedia of Victimology and Crime Prevention.* SAGE Publications, Inc.

Fissel, E. R., & Reyns, B. W. (2019). The Aftermath of Cyberstalking: School, Work, Social, and Health Costs of Victimization. *American Journal of Criminal Justice*, *45*(4), 1-18. https://pt.booksc.org/book/75924526/b15df9

Gewirtz-Meydan, A., Walsh, W., Wolak, J., & Finkelhor, D. (2018). The Complex Experience of Child Pornography Survivors. *Child Abuse & Neglect, 80,* 238-248. https://pt.booksc.org/book/69045888/3648ff

Gil, H. (2016, julho 4-6). As TIC e a Cidadania Digital 65+ [Simpósio]. Congresso Mundial de Estilos de Aprendizagem. https://repositorio.ipcb.pt/bitstream/10400.11/5364/1/As%20TIC%20e%20a%20Cidadania%20Digital%2065%2b.pdf

Gil, H. (2019). A Literacia Digital e as Competências Digitais para a Infoinclusão: por uma Inclusão Digital e Social dos Mais Idosos. *Revista de Educação a Distância e Elearning, 2*(1), 79-96. https://doi.org/10.34627/vol2iss1pp79-96

Gil, H., & Amaro, F. (2011, maio). "Currículo 'Geronto-Digital: os Idosos e a Sociedade da Informação e do Conhecimento [Sessão de Conferência].VII Conferência Internacional de TIC na Educação, Braga. https://repositorio.ipcb.pt/bitstream/10400.11/818/1/VII%20Conferencia%20Curriculo%20Geronto-Digital%20Henrique%20Gil%201021-.pdf

Gil, H., & Páscoa, G. (2018). O Bem-estar Através das Tecnologias Digitais: um Estudo em Populações 50+. *INFAD Revista de Psicología. International Journal of Developmental and Educational Psychology, 1*(2), 33-42. https://revista.infad.eu/index.php/IJODAEP/article/view/1144/1159

Grabosky, P. (2014). The Evolution of Cybercrime, 2004-2014. *RegNet Research Paper Series* (58), 1-16.

Grabosky, P. (2015). *Keynotes in Criminology and Criminal Justice Series. Cybercrime.* Oxford University Press.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). Digital Identity Guidelines. *National Institute of Standards and Technology*, *3* (4), 1-75. https://doi.org/10.6028/NIST.SP.800-63-3

Guedes, I. S., Moreira, S., & Cardoso, C. (2021). Cibercrime: Conceptualização, Desafios e Perceções Públicas. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 3-23). Pactor.

Guimarães, F. (2018). Os Mais Velhos e o Engodo das "Ciberburlas Românticas". *Jornal Público.* https://www.publico.pt/2018/02/04/sociedade/noticia/o-engodo-das-burlas-romanticas-1801709

Guinote, H. (2021). *PSP Alerta para "Ciberbullying" e Pede Atenção Parental*. Acedido em

março 27, 2022, de https://www.rtp.pt/noticias/pais/psp-alerta-para-ciberbullying-e-pede-atencao-parental_a1295812

Hadlington, L., & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice, 14*(2), 479-492. https://doi.org/10.1093/police/pay027

Halder, D. (2022). *Cyber Victimology. Decoding Cyber-crime Victimisation.* Routledge.

Hill, M. M., & Hill, A. (2016). *Investigação por Questionário.* Edições Sílabo.

HM Government. (2016). *National Cyber Security Strategy 2016 – 2021*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

Holt, T. J., Fitzgerald, S., Bossler, A. M., Chee, G., & Ng. E. (2014). Assessing the Risk Factors of Cyber and Mobile Phone Bullying Victimization in a Nationally Representative Sample of Singapore Youth. *International Journal of Offender Therapy and Comparative Criminology*, 1-18.

Instituto Nacional de Estatística. (2021). *Censos 2021*. Acedido abril 11, 2022, de https://www.ine.pt/scripts/db_censos_2021.html

International Centre for Missing & Exploited Children. (2016). *Online Child Sexual Abuse and Exploitation: Guidelines for the Adoption of National Legislation in Latin America.* https://cdn.icmec.org/wp-content/uploads/2020/09/Guidelines-for-Adoption-of-Natl-Legis-in-Latam_EN.pdf

INTERPOL. (2018). *Towards a Global Indicator on unidentified victims in child sexual exploitation material: Summary Report.* https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

INTERPOL. (2020a). *Global Landscape on COVID-19 Cyberthreat*. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

INTERPOL. (2020b). *International Child Sexual Exploitation database.* https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

INTERPOL. (s.d). *Appropriate Terminology*. https://www.interpol.int/Crimes/Crimes-against-children/Appropriate-terminology

Jansen, J., & Leukfeldt, R. (2017). Coping with Cybercrime Victimization: An Exploratory Study into the Impact and Change. *Journal of Qualitative Criminal Justice & Criminology, 6*(2), 1-30. https://www.qualitativecriminology.com/pub/v6i2p4/release/1

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy *Internet*: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice,* 1-22. https://doi.org/10.1177/10439862211027986

Khadas, H. M. (2020). The Causes of Cybercrime. *International Journal of Innovative Science and Research Technology*, *5*(8), 476-478.

Kowalski,R., Limber, S. P., & McCord, A. (2018). A Developmental Approach to Cyberbullying: Prevalence and Protective Factors. *Agression and Violent Behavior,* 1-63. https://af.booksc.eu/book/68284027/aff9f6

Kremling, J., & Parker, A. M. S. (2018). *Cyberspace, Cybersecurity, and Cybercrime*. Sage Publications, Inc.

Kuss, D. J., & Griffiths, M. D. (2011). Online Social Networking and Addiction—A Review of the Psychological Literature. *International Journal of Environmental Research and Public Health,* 8, 3528-3552.

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3194102/pdf/ijerph-08-03528.pdf

Lança, H. C. (2014). *A Regulação dos Conteúdos Disponíveis na Internet. A Imperatividade de Proteger as Crianças* [Tese de Doutoramento, Faculdade de Direito da Universidade do Porto]. Repositório Institucional do Instituto Politécnico de Beja.

Lei n.º 109/2009, de 15 de setembro. *Diário da República n.º 179/2009 - Série I.* Portugal: Assembleia da República.

Lei n.º 27/2021, de 17 de maio. *Diário da República n.º 95/2021 - Série I.* Portugal: Assembleia da República.

Lei n.º 32/2008, de 17 de junho. *Diário da República n.º 137/2008 – Série I.* Portugal: Assembleia da República.

Lei n.º 46/2018, de 13 de agosto. *Diário da República n.º 155/2018 - Série I.* Portugal: Assembleia da República.

Lei n.º 49/2008, de 27 de agosto. *Diário da República n.º 165/2008 - Série I.* Portugal: Assembleia da República.

Lei n.º 55/2020, de 23 de maio. *Diário da República n.º 167/2020 - Série I.* Portugal: Assembleia da República.

Leist, A. K. (2013). A Social Media Use of Older Adults: A Mini-Review. *International Journal of Experimental, Clinical, Behabioral and Technological Gerontology, 59*(4), 378-384. https://doi.org/10.1159/000346818

Lemos, C. F. R. C. (2019). *Uso Problemático da Internet e das Redes Rociais: Relação com a Regulação da Satisfação das Necessidades Psicológicas e a Saúde Mental* [Dissertação de Mestrado, Universidade de Lisboa: Faculdade de Psicologia]. Repositório Institucional da Universidade de Lisboa.

Leukfeldt, R., & Holt, T. J. (2020). *The Human Factor of Cybercrime.* Routledge.

Ley 9/2014, de 9 de mayo. *Boletín Oficial Del Estado n.º 114/2014*. España: Jefatura del Estado.

Lisboa, M., & Teixeira, A. L. (2015). *Policiamento de Proximidade. Representações e Práticas da População e Inovação Organizacional na Polícia.* Edições Húmus, Lda.

Litwiller, B. J., & Brausch, A. M. (2013). Cyber Bullying and Physical Bullying in Adolescent Suicide: The Role of Violent Behavior and Substance Use. *Journal of Youth and Adolescence, 42*(5), 675-684. https://pt.booksc.org/book/22023773/e2a14c

Livingstone, S. (2021). *Children's Rights Apply in the Digital World!* Blogs.lse.ac.uk. Acedido janeiro 19, 2022, de https://blogs.lse.ac.uk/medialse/2021/02/04/childrens-rights-apply-in-the-digital-world/?fbclid=IwAR0_kQjhSF2974AL2739rV2eK_GBMRcO8_tMOqJ1TWxy_r_XWuUzk6k4WzE

Loos, E. (2011). Generational Use of New Media and the (Ir)relevance of Age. In Fortunati, L. & Fausto Colombo. (Eds), *Broadband Society and Generational Changes*. (pp. 259-273). Peter Lang

Lundin, I. B. (2016). *Metodologia de Pesquisa em Ciências Sociais.* Escolar Editora.

Lusa. (2020a, setembro 16). Covid-19: Maioria dos Estudantes Foi Vítima de Bullying durante Pandemia, Diz Estudo. *Jornal Público*. https://www.publico.pt/2020/09/16/sociedade/noticia/covid19-maioria-estudantes-vitima-bullying-durante-pandemia-estudo-1931724

Lusa. (2020b). Universidade do Minho Cria 'App' para Reeducar Jovens na Denúncia das Ciberagressões. *Saúde Mais TV.* Acedido março 17, 2022, de https://saudemais.tv/noticia/21221-universidade-do-minho-cria-app-para-reeducar-jovens-na-denuncia-das-ciberagressoes

Ly, T., Dwyer, R. G., & Fedoroff, J. P. (2018). Characteristics and Treatment of *Internet*

Child Pornography Offenders. *Behavioral Sciences & the Law, 36*(2), 216-234. https://pt.booksc.org/book/69379454/b6c16b

Machado, P. D. D. (2015). *O Papel da GNR no Contexto da Cibersegurança Nacional* [Trabalho de Investigação Individual do CEMC, Instituto de Estudos Superiores Militares]. Repositório Científico de Acesso Aberto de Portugal.

Maia, C. M. T. (2019). *Ciberpoliciamento das Redes Sociais: O Contributo das Ciências Tecnológicas* [Estudo Teórico, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Científico de Acesso Aberto de Portugal.

Malwarebytes. (s.d). *What is Phishing?*. Acedido outubro 25, 2021, de https://www.malwarebytes.com/phishing

March, E., Litten, V., Sullivan, D. H., & Ward, L. (2020). Somebody that I (used to) Know: Gender and Dimensions of Dark Personality Traits as Predictors of Intimate Partner Cyberstalking. *Personality and Individual Differences, 163*, 1-6. https://pt.booksc.org/book/82097408/dd174f

Marconi, M. A., & Lakatos, E. M. (2017). *Fundamentos da Metodologia Científica.* (8ª ed.). Editora Atlas S.A.

Marcum, C. D., Higgins, G. E., & Nicholson, J. (2017). Crossing Boundaries Online in Romantic Relationships: An Exploratory Study of The Perceptions of Impact on Partners by Cyberstalking Offenders. *Deviant Behavior,* 1-16. https://pt.booksc.org/book/67135428/0c3570

Marczak, M., & Coyne, I. (2015). A Focus on Online Bullying. In Atrill, A. (2015). *Cyberpsychology*. Oxford.

Martellozzo, E., & Jane, E. A. (2017). *Cybercrime and its Victims.* Routledge.

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S., & Lupu, E. (2019). Introduction. In Rashid, M. A. S. A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (Eds.), *The Cyber Security Body of Knowledge*. CyBOK. (p. 3). https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf

Martins, A. M. R. (2018). Sentimento de Insegurança e Vitimação no Ciberespaço: a Relação entre Variáveis Individuais e Contextuais [Dissertação de Mestrado, Faculdade de Direito da Universidade do Porto]. Repositório Aberto da Universidade do Porto.

McConnell International. (2000). *Cyber Crime…and Punishment? Archaic Laws Threaten Global Information*. https://uh.edu/tech/cisre/resources/ia-resources/_files/7033/Week12/cybercrime.pdf

Mendes, B. S. A. (2014). *Profiling Criminal: Técnica Auxiliar de Investigação Criminal* [Dissertação de Mestrado, Universidade do Porto: Instituto de Ciências Biomédicas Abel Salazar]. Repositório Aberto da Universidade do Porto.

Mendonça, P. (2021, dezembro 14). Conceitos e Ecossistema de Cibersegurança [Apresentação]. Curso Geral de Cibersegurança. https://www.cncs.gov.pt/pt/curso-geral-ciberseguranca/

Militão, O. P. (2014). *Guerra da Informação: a Cibersegurança, a Ciberdefesa e os Novos Desafios Colocados ao Sistema Internacional* [Dissertação de Mestrado, Universidade Nova de Lisboa, Faculdade de Ciências Sociais e Humanas]. Repositório da Universidade Nova de Lisboa.

Miró-Llinares, F. (2015). That Cyber Routine, That Cyber Victimization: Profiling Victims of Cybercrime. In Smith, R. G., Cheung, R. C., & Lau, L, Y. (Eds.), *Cybercrime Risks and Responses. Eastern and Western Perspectives.* (pp. 71-86). Palgrave Macmillan.

N. B. M. (2012). Crimes na *Internet*. *Revista Polícia Portuguesa, 003*(4), 22.

National Crime Agency. (2020). *National Strategic Assessment of Serious and Organised Crime.* https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file

Navarro, R., Yubero, S., & Larrañaga, E. (2016). *Cyberbullying Across the Globe: Gender, Family, and Mental Health.* Springer.

Nobles, M., Reyns, B. W., Fox, K., & Fisher, B. S. (2014). Protection Against Pursuit: A Conceptual and Empirical Comparison of Cyberstalking and Stalking Victimization Among a National Sample. *Justice Quarterly, 31*(6). 1-40. https://keep.lib.asu.edu/_flysystem/fedora/c160/Protection_Against_Pursuit.pdf

Nunes, D. R. (2021). *Os Meios de Obtenção de Prova Previstos na Lei do Cibercrime*. (2ªed.). GESTLEGAL.

O´Shea, B., Julian, R., Prichard, J., & Kelty, S. (2019). Challenges in Policing Cyberstalking:A Critique of the Stalking Risk Profile in the Context of Online Relationships. In Lumsden, K & Harmer, E. (Eds.), *Online Othering: Exploring Digital Violence and Discrimination on the Web*. (pp. 331-353). Palgrave Studies in Cybercrime and Cybersecurity.

Ofcom. (2020). *Children and Parents: Media Use and Attitudes Report 2019*. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf

Oksanen, A., & Keipi, T. (2013). Young People as Victims of Crime on the *Internet*: A Population-based Study in Finland. *Vulnerable Children and Youth Studies, 8*(4), 298–309. https://pt.booksc.org/book/41640050/b6b42b

Oliveira, J. F. (2002). *As Políticas de Segurança e os Modelos de Policiamento* [Dissertação de Mestrado, Instituto Superior de Ciências do Trabalho e da Empresa].

Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2018). *A Global Framework of Reference on Digital Literacy Skills for Indicator 4.4.2.* http://uis.unesco.org/sites/default/files/documents/ip51-global-framework-reference-digital-literacy-skills-2018-en.pdf

Patrão, I. (2019). *Guia: Dependências Online*. *Orientações para a Gestão Saudável dos Comportamentos Online*. https://www.*internet*segura.pt/sites/default/files/2020-04/Centro_*Internet*_Segura_Guia_Depend%C3%AAncias_Online.pdf

Patrão, I., Fernandes, P. A., & Enes-Pinheiro, B. (2021). "A *INTERNET* VAI À ESCOLA": Como Promover o Uso Saudável das Tecnologias Digitais em Crianças dos 3 aos 6 anos. In Dias, P., & Brito. R. *DIGIKIDS: a Utilização de Tecnologias Touchscreen por Crianças até aos 6 Anos*. (pp. 144-161). Centre for Psychological, Family and Social Wellbeing (CRC-W).

Patrão, I., Machado, M., Fernandes, P. A., & Leal, I. (2012). Jovens e *Internet*: Relação com o Bem-estar Psicológico, Isolamento Social e Funcionamento Familiar. *Actas do 13º Colóquio de Psicologia e Educação,* 241-249. https://repositorio.ispa.pt/bitstream/10400.12/5537/1/CPE_15_241-249.pdf

Paulus, F. W., Ohmann, S., Gontard, A.V., & Popow. C. (2018). *Internet* Gaming Disorder in Children and Adolescents: a Systematic Review. *Develpmental Medicine & Child Neurology, 60* (7), 645-659. https://onlinelibrary.wiley.com/doi/full/10.1111/dmcn.13754

Poiares, N. (2019). Cibersegurança, Literacia e Resiliência Digital dos Idosos. *Anuário Janus 2018-2019: A Dimensão Externa da Segurança Interna,* (19), 118-119. https://comum.rcaap.pt/bitstream/10400.26/35402/1/Janus19_2_23_Nuno%20Poiares_Ciberseguran%c3%a7a%20%281%29.pdf

Poiares, N. (2020). Violência Doméstica e Redes Sociais: A Proteção Jurídico-Penal da Vida Privada na *Internet*. *Cyber Law by CIJIC,* (10), 10-59. https://comum.rcaap.pt/bitstream/10400.26/34815/1/Violencia-domestica-a-protecao-juridico-penal-da-vida-privada-na-*internet*.pdf

Ponte, C., Ferreira, E., Cardoso, D., Batista, S., Brito, R., Simões, J. A., Senne, F., Castro, T.

S., Dias, P., & Cruz, R. M. (2020). *Nós na Rede: Ambientes Digitais de Crianças e Jovens*. Edições Almedina, S.A.

PORDATA. (2021). Indivíduos com 16 e mais Anos que Utilizam Computador e *Internet* em % do Total de Indivíduos: por Grupo Etário. https://www.pordata.pt/Portugal/Indiv%C3%ADduos+com+16+e+mais+anos+que+utilizam+computador+e+*Internet*+em+percentagem+do+total+de+indiv%C3%ADduos+por+grupo+et%C3%A1rio-1139

Portal da Queixa. (2022). *Dia Mundial do Consumidor: O quão Seguros Online estão os Consumidores Portugueses*. Acedido março 24, 2022, de https://portaldaqueixa.com/news/seguranca-online-consumidores-portugueses

Ramalho, S. C. (2021). A Utilização de Tecnologias *Touchscreen* por Crianças até aos 6 Anos: Breve Olhar da Psicologia do Desenvolvimento. In Dias, P., & Brito. R. *DIGIKIDS: a Utilização de Tecnologias Touchscreen por Crianças até aos 6 Anos*. (pp. 12-34). Centre for Psychological, Family and Social Wellbeing (CRC-W).

Ramos, A. D. (2022). *O Agente Encoberto Digital. Meios especiais e técnicos de investigação criminal.* Almedina.

Reis, F. L. (2018). *Investigação Científica e Trabalhos Académicos: Guia Prático.* Edições Sílabo.

Resolução do Conselho de Ministros n.º 92/2019. *Diário da República n.º 108/2019- Série I.* Portugal: Presidência do Conselho de Ministros.

Robalo, T. L. A. S. (2021). Cibervitimação e Teorias Criminológicas Relevantes. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 37-51). Pactor.

Rosenbaum, D. & Lurigio, A. (1994). An Inside Look at Community Policing Reform: Definitions, Organizational Changes, and Evaluation Findings. *Crime & Delinquency, 40*(3), 299-314. https://pt.booksc.org/book/23327120/686219

Sani, A. I., & Valquaresma, J. (2020). Cyberstalking: Prevalência e Estratégias de Coping em Estudantes Portugueses do Ensino Eecundário. *Avances en Psicología Latinoamericana*, *38*(3), 1-18. https://doi.org/10.12804/revistas.urosario.edu.co/apl/a.8160

Sani, A. I., Carrasquinho, J., & Soeiro, C. (2018). Violência nas Relações de Intimidade em Jovens e os Comportamentos de *Stalking* e *Ciberstalking*. In Paulino, M. & Alchieri, J. C. (Coords.), *Desvio, Crime e Vitimologia*. (pp. 71-85). Pactor.

Santo, P. E. (2015). *Introdução à Metodologia das Ciências Sociais: Génese, Fundamentos e Problemas.* Edições Sílabo.

Santos, D. (2020). A Pandemia de COVID-19 e os Ciberataques em Portugal. *IDN Brief*, 32, 3-4. https://comum.rcaap.pt/bitstream/10400.26/33350/1/Cibersegurancaeciberdefesaemtemposdepandemia_IDNBrief_N_32_Julho_2020.pdf

Santos, G., Santos, M., Gaffney, H., & Farrington, D. P. (2021). Cyberbullying: Da Conceptualização à Prevenção. Uma Revisão Teórica. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 135-157). Pactor.

Santos, L., & Guedes, A, M. (2015). Breves reflexões sobre Poder e Ciberespaço. *Revista de Direito e Segurança, 6*, 189-209. https://comum.rcaap.pt/bitstream/10400.26/14329/1/PodereCiberesa%C3%A7o.pdf

Santos, P., & Manteigas, J. (2010). *Internet Segura para Crianças. Guia para Pais e Educadores*. FCA.

Santos, P., Bessa, R., & Pimentel, C. (2008). *Cyberwar: o Fenómeno, as Tecnologias e os Actores.* FCA.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses.* Universidade Lusíada Editora.

Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências. (2018). *Comportamentos Aditivos aos 18 anos: Inquérito aos Jovens Participantes no Dia da Defesa Nacional – 2018.* https://www.cnpdpcj.gov.pt/documents/10182/14804/Comportamentos+Aditivos+aos+18+Anos/fd0085bd-bbb6-4c46-916a-33828d7b9f8b

Serviço de Intervenção nos Comportamentos Aditivos e nas Dependências. (2019). *Jogo, Internet e Outros Comportamentos Aditivos. Dossier Temático.* https://www.sicad.pt/BK/EstatisticaInvestigacao/EstudosConcluidos/Lists/SICAD_ESTUDOS/Attachments/201/DossierJogo*Internet*OutrosCA_PT.PDF

Severino, A. J. (2017). *Metodologia do Trabalho Científico.* (24ª ed.). Cortez Editora.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar. What Everyone Needs to Know.* Oxford University Press.

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrdu, E., Ólafsson, K., Livingstone, S., & Hasebrink, U. (2020). *EU Kids Online 2020: Survey Results from 19 Countries.* EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Smith, P. K. (2013). Cyberbullying y Ciberagresión. In Ovejero, A., Smith, P. K., & Yubero, S. (Coords.), *El Acoso Escolar y su Prevención. Perspectivas Internacionales.* (pp.173-189). Biblioteca Nueva.

Spiegel, M. R., & Stephens, L. J. (2009). *Estatística*. (4ªed.). Bookman.

Stainer, P. (2021, Maio 04). *Alarming Cybersecurity Statistics for 2021 and the Future*. Retarus corporate blog. https://www.retarus.com/blog/en/alarming-cybersecurity-statistics-for-2021-and-the-future/

Stochemer, D. (2019). *Quantitative Methods for the Social Sciences. A Practical Introduction with Examples in SPSS and Stata.* Springer.

Terre des Hommes. (2018). *The Dark Side of the Internet for Children: Online Child Sexual Exploitation in Kenya. A rapid Assessment Report.* https://www.datocms-assets.com/22233/1600704755-tdh-nl-ocse-in-kenya-research-report-feb-2018.pdf

Thakur, K., & Pathan, A. K. (2020). *Cybersecurity Fundamentals. A Real-World Perspective.* CRC Press.

Thompson, F., & Smith, P. K. (2013). Estrategias *Antibullying* Dentro de los Centros: lo que se Hace y lo que Funciona. In Ovejero, A., Smith, P. K. & Yubero, S. (Coords.), *El Acoso Escolar y su Prevención. Perspectivas Internacionales.* (pp.241-262). Biblioteca Nueva.

Tilley, N. (2005). *Handbook of Crime Prevention and Community Safety.* Willan Publiching.

Todd, C., Bryce, J., & Franqueira, V. N. L. (2020). Technology, Cyberstalking and Domestic Homicide: Informing Prevention and Response Strategies. *Policing and Society, 31*(1), 1-18. https://pt.booksc.org/book/83023154/c3cb88

Tokunaga, R. S. (2010). Following you Home from School: A Critical Review and Synthesis of Research on Cyberbullying Victimization. *Computers in Human Behavior, 26*, 277-287. https://eclass.uoa.gr/modules/document/file.php/PPP357/Following%20you%20home%20from%20school%20A%20critical%20review%20and%20synthesis%20of%20research.pdf

União de Mulheres Alternativa e Resposta (UMAR). (2019). *Estudo Nacional sobre a Violência no Namoro 2019.* http://www.umarfeminismos.org/images/stories/noticias/Estudo_Nacional_VN_2019_da_UMAR.pdf

United Nations International Children´s Emergency Fund. (2017). *The State of the World´s*

Children 2017: Children in a Digital World. UN-iLibrary. https://www.un-ilibrary.org/content/books/9789213630679/read

United Nations International Children´s Emergency Fund. (2019). *Growing Up in a Connected World.* Office of Research – Innocenti. https://www.unicef-irc.org/publications/pdf/GKO%20Summary%20Report.pdf

Vale, M., Matos, M., & Pereira, F. (2021). Ciberabuso nas Relações de Intimidade dos Adolescentes: Um Diálogo entre a Psicologia e a Criminologia. In Guedes, I. S. & Gomes, M. A. M. (Coords), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 119-133). Pactor.

Vara, M., & Sani, A. I. (2021). Pornografia Infantil: (Re)conhecimento e Prevenção Criminal do Fenómeno. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade: Novos Desafios, Ofensas e Soluções*. (pp. 99-117). Pactor.

Venâncio, P. D. (2021). Tipos Legais de Crimes Informáticos. In Guedes, I. S. & Gomes, M. A. M. (Coords.), *Cibercriminalidade. Novos Desafios, Ofensas e Soluções.* (pp. 75-97). Pactor.

Verdelho, P. (2016). Cibercrime no Ambiente Escolar [Webinar]. Direção Geral da Educação. https://webinars.dge.mec.pt/webinar/cibercrime-no-ambiente-escolar

Verdelho, P., Bravo, R., & Rocha, M. L. (2003). *Leis do Cibercrime*. *Volume 1*. Centro Atlântico.

Villora, B., Navarro, R., & Yubero, S. (2019). The Role of Social-Interpersonal and Cognitive-Individual Factors in Cyber Dating Victimization and Perpetration: Comparing the Direct, Control, and Combined Forms of Abuse. *Journal of Interpersonal Violence, 36*(2), 1-26. https://www.researchgate.net/publication/333459823_The_Role_of_Social-Interpersonal_and_Cognitive-Individual_Factors_in_Cyber_Dating_Victimization_and_Perpetration_Comparing_the_Direct_Control_and_Combined_Forms_of_Abuse

Virtanen, S. (2017). Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. https://pt.booksc.org/book/66044208/a8ae4d

Weber, N. L., & Pelfrey, W. V. (2014). *Cyberbullying: Causes, Consequences, and Coping Strategies.* LFB Scholarly Publishing LLC.

Williams, M. L. (2015). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *The British Journal of Criminology, 56*(1), 21-48. https://academic.oup.com/bjc/article/56/1/21/2462277

Worsley, J. D., Wheatcroft, J. M., Short, E., & Corcoran, R. (2017). Victims' Voices: Understanding the Emotional Impact of Cyberstalking and Individuals' Coping Responses. *SAGE journals,* 1-13. https://journals.sagepub.com/doi/10.1177/2158244017710292

Yu, S. (2014). Fear of Cyber Crime Among College Students in the United States: An Exploratory Study. *International Journal of Cyber Criminology,8*(1), 36-46. https://www.cybercrimejournal.com/yuijcc2014vol8issue1.pdf

Yubero, S., Larrañaga, E., & Martínez, I. (2013). Familia, Comunicación y Conductas de Acoso. In Ovejero, A., Smith, P. K. & Yubero, S. (Coords.), *El Acoso Escolar y su Prevención. Perspectivas Internacionales.* (pp.209-225). Biblioteca Nueva.

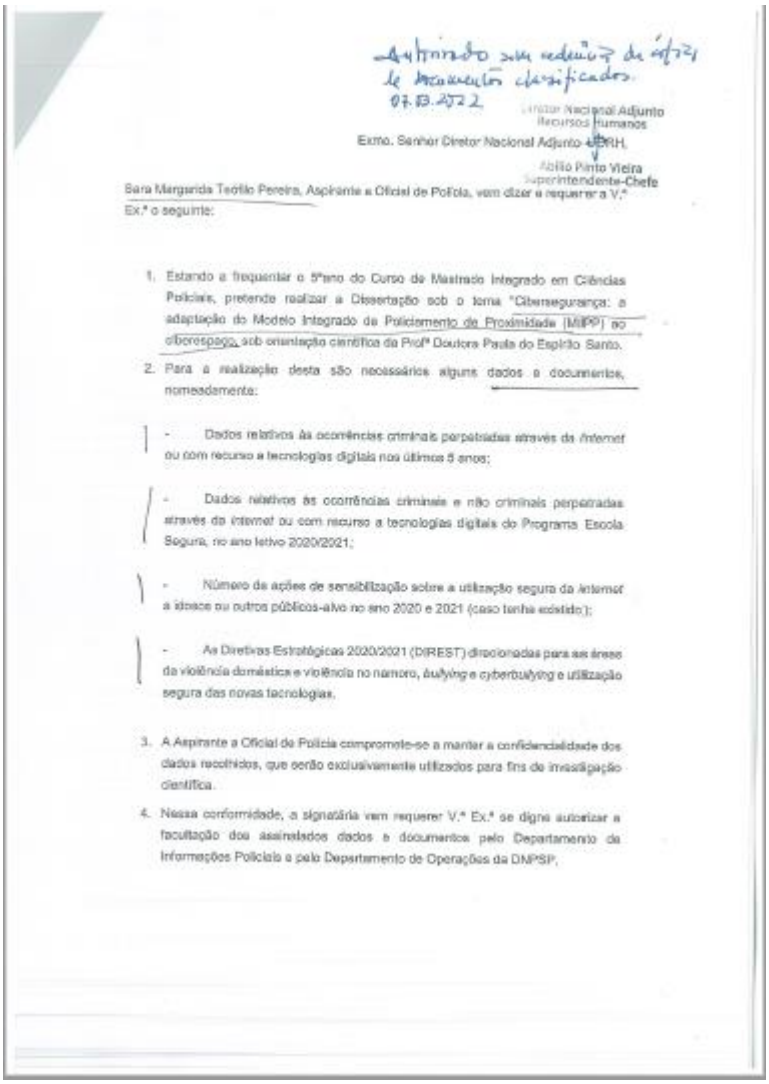
Zilka, G. C. (2017). Awareness of Esafety and Potential Online Dangers Among Children and Teenagers. *Journal of Information Technology Education: Research, 16*, 319-338. Awareness of eSafety and Potential Online Dangers among Children and Teenagers (jite.org)

Zweig, J, M., Dank, M., Yahner, J., & Lachman, P. (2013b). The Rate of Cyber Dating Abuse Among Teens and How It Relates to Other Forms of Teen Dating Violence. *Journal of Youth Adolescence, 42*(7), 1063-1077.

Zweig, J. M., Lachman, P., Yahner, J., & Dank, M. (2013a). Correlates of Cyber Dating Abuse Among Teens. *Journal of Youth Adolescence, 43*(8), 1306-1321.

Apêndices

Apêndice A- Autorização para acesso a informação



Autorizado sem redução de âmbito de documentos classificados.
07.03.2022

Diretor Nacional Adjunto
Recursos Humanos

Exmo. Senhor Diretor Nacional Adjunto de RH,

Abílio Pinto Vieira
Superintendente-Chefe

Sara Margarida Teófilo Pereira, Aspirante a Oficial de Polícia, vem dizer e requerer a V.ª Ex.ª o seguinte:

1. Estando a frequentar o 5º ano do Curso de Mestrado Integrado em Ciências Policiais, pretende realizar a Dissertação sob o tema "Cibersegurança: a adaptação do Modelo Integrado de Policiamento de Proximidade (MIPP) ao ciberespaço, sob orientação científica da Profª Doutora Paula do Espírito Santo.
2. Para a realização desta são necessários alguns dados e documentos, nomeadamente:

- Dados relativos às ocorrências criminais perpetradas através da Internet ou com recurso a tecnologias digitais nos últimos 5 anos;
- Dados relativos às ocorrências criminais e não criminais perpetradas através da Internet ou com recurso a tecnologias digitais do Programa Escola Segura, no ano letivo 2020/2021;
- Número de ações de sensibilização sobre a utilização segura da Internet a idosos ou outros públicos-alvo no ano 2020 e 2021 (caso tenha existido);
- As Diretivas Estratégicas 2020/2021 (DIREST) direcionadas para as áreas da violência doméstica e violência no namoro, bullying e cyberbullying e utilização segura das novas tecnologias.

3. A Aspirante a Oficial de Polícia compromete-se a manter a confidencialidade dos dados recolhidos, que serão exclusivamente utilizados para fins de investigação científica.
4. Nessa conformidade, a signatária vem requerer V.ª Ex.ª se digne autorizar a facultação dos assinalados dados e documentos pelo Departamento de Informações Policiais e pelo Departamento de Operações da DMPSP.

Apêndice B- Termos de consentimento informado dos informadores qualificados

Informador Qualificado 1

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

O Informante Privilegiado

Assinado por: **Nelson José Roque Amador**
Num. de Identificação: 12286868
Data: 2022.04.13 12:54:25+01'00'

CHAVE MÓVEL

Informador Qualificado 2

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

O Informante Privilegiado

Sónia Alexandra Fonseca Martins

Comissário, M/152675

1

Informador Qualificado 3

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

O Informante Privilegiado

Rui Filipe Lourenço Santos Costa
Subintendente

1

Informador Qualificado 4

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

Assinada por: Nuno Caetano Lopes de Barros Pelares
Identificação: BI10124621
Data: 2022-04-13 às 11:42:34

1

Informador Qualificado 5

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

O Informante Privilegiado

Hugo Duarte de Sousa Batista e Guinote

Hugo Duarte de Sousa Batista e Guinote

Intendente M/100222

1

Informador Qualificado 6

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

Termo de Consentimento Informado

(Entrevista)

Serve o presente documento como vinculação à Dissertação de Mestrado com o título "Cibersegurança: o papel da PSP na prevenção do cibercrime" elaborada pela Aspirante a Oficial de Polícia Sara Margarida Teófilo Pereira, M/157271, aluna do Mestrado Integrado em Ciências Policiais do Instituto Superior de Ciências Policiais e Segurança Interna.

Foram-me explicados os objetivos da realização desta entrevista assim como me foi informado de que iria ser gravada, sendo os registos destruídos aquando do seu tratamento. A minha participação neste estudo tem caráter voluntário e as respostas fornecidas serão utilizadas exclusivamente para fins de investigação científica.

Neste sentido, consinto que os dados produzidos, através desta entrevista, assim como a minha identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo.

O Informante Privilegiado

Apêndice C- Autorização para a realização das entrevistas

Autorizados os diversos pedidos anexos. Os documentos reservados ou classificados serão apenas consultados não sendo cedidas cópias.

DN DEPFORM

19 JAN. 2022

De: ISCPSI - Direcção Ensino
Enviado: terça-feira, 18 de janeiro de 2022 15:15
Para: DN DEPFORM
Cc: Nuno Ricardo Pica Dos Santos; Sergio Do Rosario Cruz
Assunto: PEDIDOS DE COLABORAÇÃO EM TRABALHOS DE DISSERTAÇÕES DE MESTRADOS INTEGRADOS EM CIÊNCIAS POLICIAIS
Anexos: 28SECDE2022.pdf; 29SECDE2022.pdf; 5SECDE2022.pdf; 31SECDE2022.pdf; 8SECDE2022.pdf; 7SECDE2022.pdf; 11SECDE2022.pdf; 17SECDE2022.pdf; 10SECDE2022.pdf; 9SECDE2022.pdf; 12SECDE2022.pdf; 14SECDE2022.pdf; 16SECDE2022.pdf; 15SECDE2022.pdf; 13SECDE2022.pdf; 18SECDE2022.pdf

DIRETOR NACIONAL

Exmo. Senhor
Diretor do Departamento de Formação
Mi. Superintendente Paulo Onofre

Manuel A[illegible] da Silva
Sup[illegible]

Relativamente ao assunto em epígrafe, encarrega-me o Exmo. Sr. Diretor de Estágio, Subintendente Nuno Pica dos Santos, de enviar a V.Ex.ª os ofícios n.ºs 5; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16; 17; 18; 28; 29 e 31/SECDE/2022 em anexo, referente aos alunos do 34.º CFOP.

Sem mais assunto e com os melhores cumprimentos,

"Uma Polícia integral, humana, forte, coesa e ao serviço do Cidadão" – Estratégia PSP 20/22

Joaquim Augusto Leite Veiga
Diretor de Ensino

POLÍCIA

Instituto Superior de Ciências Policiais e Segurança Interna

DIRECÇÃO NACIONAL DA P.S.P.
DEPARTAMENTO DE FORMAÇÃO
Entrada Nº 167 Processo Nº 3706
Data 19/1/2022

1

Apêndice D- Autorização da Direção do Agrupamento de Escolas Marcelino Mesquita

REPÚBLICA PORTUGUESA | EDUCAÇÃO

Para:
Sara Margarida Teófilo Pereira
Rua Cap. Salgueiro Maia, nº10, 1ºDtº

2070 – 064 Cartaxo

N/ referência:	S/ comunicação de:	N/ referência:	Data
		125-2	2022/03/10

ASSUNTO: ***Autorização de aplicação de questionários***

No seguimento do pedido da mestranda do Instituto Superior de Ciências Policiais e Segurança Interna, **Sara Margarida Teófilo Pereira**, para aplicar um questionário aos alunos da Escola Básica José Tagarro, pertencente ao Agrupamento de Escolas Marcelino Mesquita do Cartaxo, vem esta Direção autorizar a referida solicitação.

Com os melhores cumprimentos,

O Diretor

Dr. Jorge Tavares

Sede: Agrupamento de Escolas Marcelino Mesquita do Cartaxo - Travessa Valmosqueiro s/n – 2070-147 Cartaxo
Escola Secundária do Cartaxo - José Ribeiro da Costa, S/N, 2070-099 Cartaxo
NIF: 600079791

Apêndice E- Autorização da Direção do Agrupamento de Escolas Moinhos da Arroja

De: Paula Fernanda Diogo de Oliveira [mailto:paulaoliveira@aemoinhosarroja.pt]
Enviada: 25 de março de 2022 13:04
Para: Sara Margarida Teofilo Pereira; Paulo Bernardo
Assunto: Re: Pedido de autorização de aplicação de questionários

Atenção: Este email foi originado fora da RNSI. Por favor, não clique em links nem abra anexos, a não ser que conheça o remetente e saiba que o seu conteúdo é seguro.

Exma. Sra.,

É autorizada a aplicação dos questionários na escola EB1/JI Manuel Coco.

Vai ser enviada o nº de turmas e de alunos em cada uma delas.

Votos de um bom trabalho!

Com os melhores cumprimentos,

Paula Diogo de Oliveira (PhD)

Adjunta do Diretor

AGRUPAMENTO DE ESCOLAS
MOINHOS DA ARROJA

Agrupamento de Escolas Moinhos da Arroja

Rua Fernando Lopes Graça,

Urbanização da Arroja - 2675-549 Odivelas
Tel.: 21 934 88 50

www.aemoinhosarroja.pt/

https://moodle.aemoinhosarroja.pt/

Apêndice F- Guião da entrevista

Guião da Entrevista

Este guião foi criado no âmbito da realização da Dissertação de Mestrado Integrado em Ciências Policiais, subordinada ao tema "Cibersegurança: o papel da Polícia de Segurança Pública na prevenção do cibercrime". No presente trabalho adotar-se-á uma metodologia qualitativa, recorrendo a entrevistas semiestruturadas como instrumento de recolha de dados. As respostas fornecidas são **confidenciais** e serão exclusivamente utilizadas para fins de investigação científica.

Consente que os dados produzidos, através desta entrevista, assim como a sua identidade, sejam citados para fins académicos, no âmbito do trabalho que está a ser produzido pela autora deste estudo, no ISCPSI?

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?
2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?
3. Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?
4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?
5. Quanto controlo *online* é necessário e quando é demasiado?
6. Em relação ao MIIP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?
7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.
8. Quais os riscos que correm as crianças ao navegar na *internet*?
9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

Apêndice G- Transcrições das entrevistas

Informador qualificado 1

Cargo: Agente Principal, especialista/mestre em cibercrime

Data: 17 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: A PSP tem um papel fundamental na prevenção do cibercrime, mas em primeiro lugar temos de falar nas medidas preventivas. A PSP tem tido um papel ativo nas redes sociais, nos meios de comunicação social nos últimos anos relativamente às questões que podem fazer perigar aos utilizadores da *internet* e nomeadamente falo nas campanhas de sensibilização, de informação. As divulgações são feitas normalmente nas redes sociais. Ainda há poucos dias, a situação do *phishing*: supostas entidades que se fazem passar por outras. Todo esse tipo de prevenção é importante, importante alertar a população. Temos de vincar é os riscos existentes que representam o descuro na utilização das novas tecnologias e da *internet*. O combate é outra questão, julgo que a PSP tem outro papel, na minha opinião, neste momento, o que não quer dizer que no futuro não possa mudar, mas neste momento é mais na vertente preventiva, não tanto na parte do combate em si, é mais no combate na investigação desse tipo de criminalidade.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: Através de uma cada vez melhor e maior formação e especialização dos polícias que trabalham nessa área. A capacidade de investigar, neste momento temos de fazer uma divisão: a criminalidade que foi transposta do mundo virtual para o mundo real, que é toda a panóplia de crimes que nós temos no código penal e depois temos aquela parte mesmo da criminalidade informática que, deve começar, e se olharmos para as competências legais conferidas à PSP através da LOIC, esse tipo de criminalidade é de competência exclusiva da PJ. Mas não quer dizer que os nossos profissionais não tenham que estar preparados para enfrentar a criminalidade, nomeadamente através de uma monitorização do ciberespaço, particularmente das redes sociais e de outro tipo de locais que são disponíveis na *internet* de acesso livre ao cidadão mas também tem de haver uma especialização para que tenhamos cada vez mais profissionais que conseguem entrar no chamado *dark web*, que é onde nós podemos encontrar mais criminalidade, aquilo que nos interessa mais na nossa profissão que é prevenir a criminalidade que mais preocupa a população. Também temos de ter em atenção que tem de haver uma cooperação cada vez maior entre as entidades responsáveis pela investigação do cibercrime e as empresas responsáveis pelo armazenamento dos dados de tráfego. A matéria de investigação criminal do cibercrime está muito dependente ainda daqueles. Não nos podemos esquecer que o cidadão deve estar cada vez mais sensibilizado para a importância de denunciar os crimes e, por vezes o setor empresarial não faz tanto como devia fazer, não quer vincular uma imagem de vulnerabilidade e de não terem capacidade de as suas empresas assegurarem uma cibersegurança perante a opinião pública que devia ser o máximo dos máximos.

3. Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: Embora não tenha conhecimento direto da atividade desenvolvida pelo Gabinete de cibercriminalidade da PSP. Neste papel apenas posso dar a minha opinião, que é baseada nas leituras que tenho feito ao longo dos tempos: é indiscutível que o ciberespaço deve ser alvo de uma monitorização recorrente, nas fontes mais disponíveis, abertas ao público; a monitorização das atividades, das redes sociais; a possibilidade de capacidade técnica dos investigadores a descerem até à camada mais obscura da *internet*. O policiamento é muito diferente daquilo que nós conhecemos nas cidades. No policiamento preventivo é mais difícil de atuar, tem de haver uma adaptação que sinceramente não conheço qual é o papel da PSP no gabinete mas deve passar por muito pela monitorização do ambiente digital, pela criação de mais informação, transmitir aquilo que tem de transmitir aos profissionais para nós estarmos também mais alerta às situações que podem perigar na *internet* e podem fazer com que as populações estejam mais desprotegidas.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R: O ciberespaço já por si é um ambiente particular, a monitorização deve ter em conta essa particularidade. Não podemos patrulhar o ciberespaço da mesma forma como patrulhamos uma cidade. Em primeiro lugar porque o ciberespaço na sua definição prima é o espaço virtual, não tem fronteiras que permitam delimitar um espaço, que é virtual, portanto será difícil estabelecer uma consideração de uma jurisdição.

Podemos falar apenas do ciberespaço de interesse nacional. Está relacionado com a disponibilidade, a integridade e confidencialidade de toda uma estrutura interconectada e as infraestruturas vitais para a nossa nação. As particularidades são essas. Temos de ter em conta da particularidade do ambiente ciber.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: O controlo online é necessário, não há volta a dar. Demasiado? Julgo que não é demasiado se não suspeitar contra as liberdades das pessoas, portanto esse controlo é necessário, é inevitável. Para o bem da segurança e do funcionamento do nosso país, isso não há volta a dar.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: Na parte do MIPP, da Escola segura e do programa de apoio a idosos que, para mim são as valências que mais tem contribuído para sensibilizar as camadas mais vulneráveis. Não tenho conhecimento se existem programas também a nível de *internet*, julgo que já vi alguma coisa em tempos também para sensibilização dos mais idosos. Limitações, não vejo aqui, talvez não sejam feitas ações suficientes atualmente. São duas valências dos MIPP que devem continuar a apostar nessa vertente preventiva, informativa, de sensibilizar todos os utilizadores, nomeadamente os mais jovens junto das escolas e os mais idosos também, que cada vez mais utilizam a *internet* para todo o tipo de utilidade (comunicar com a família, etc.), como qualquer outra pessoa.

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: Publico alvo: crianças, jovens e idosos. Vamos fazer um pouco aqui a ligação com outra questão. As crianças têm de ser sensibilizadas para os perigos que existem na utilização da *internet* e os idosos também para serem informados e alertados para como devem proceder e se comportar na utilização desta fantástica ferramenta que veio alterar por completo a nossa sociedade. Os jovens e os idosos são uma camada mais importante a sensibilizar neste momento.

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: Estarem sujeitos a conteúdos inadequados para a idade, por exemplo, aos *phishings*, burlas, *cyberbullying*, predadores sexuais, nomeadamente também fazerem *download* de programas que podem conter *malware* ou programas que estão sujeitos a direitos de autor são os conteúdos que mais preocupam os pais e a Polícia neste caso, que possam pôr em risco as nossas crianças quando navegam na *internet*. Este tipo de problemas…os predadores sexuais, que atrás do computador não se consegue, a pessoa pode dizer que tem15, 16 anos e afinal tem 35, e pode levar as crianças a determinados comportamentos que podem pôr os menores em risco.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: No futuro que já está cá. Com a quarta revolução industrial, com o 5G, portanto toda a interconectividade dos sistemas (os veículos interconectados, as casas, todo o tipo de material conectado que não estando protegido o suficiente pode pôr em risco a população; as fake news; os algoritmos, ainda há pouco tempo vimos uma imagem de uma manifestação de um político que julgo que era dinamarquês, em que foi visto sem máscara de proteção, isso foi tudo uma montagem…isso é o futuro, e a preocupação com a 5G, o tempo de latência vai diminuir, vai ser muito preocupante para as equipas de cibersegurança, para as equipas que investigam este tipo de criminalidade, para a PSP (imaginemos um ataque a larga escala onde por exemplo deixa-se de ter energia numa cidade que pode levar ao caos numa cidade). São esses os desafios para mim mais importantes a nível da cibercriminalidade nos próximos anos.

Informador qualificado 2

Cargo: Comissário, Chefe do Núcleo de Cibercriminalidade do DIC

Data: 10 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: O Núcleo de Cibercriminalidade deve ser o Núcleo mais recente da PSP, já estava previsto desde 2017, mas só foi implementado em novembro de 2020 e começámos efetivamente a prestar apoio à estrutura de Investigação Criminal em janeiro de 2021, portanto tem um ano e pouco de existência. Quando foi estipulada a criação do Núcleo, estava previsto no despacho que a missão deste era dar apoio à estrutura de IC no âmbito da prevenção, deteção e investigação de crimes da competência da PSP que contam com o auxílio de meios informáticos para serem cometidos. A PSP não atua em todo o tipo de cibercriminalidade. Existem dois tipos de cibercrime: os crimes ciber-instrumentais e os crimes ciber-dependentes, sendo que a PSP atua nos primeiros, ou seja, nos crimes ditos tradicionais, mas que contam com o auxílio de plataformas na *internet* ou às redes sociais ou a mensagens de correio eletrónico para serem cometidos. Ou seja, são aqueles crimes praticados no ciberespaço mas contra bens jurídicos que não são digitais, contra bens jurídicos por exemplo como a honra ou a imagem. São crimes tradicionais, mas que agora recorrem a novos métodos para serem cometidos, por exemplo, um dos mais recorrentes, que recebemos mais denúncias, são as burlas por meio da *internet*. Os outros crimes que ocorrem também no ciberespaço, designados ciber-dependentes, são aqueles que atacam a confidencialidade, a integridade, a disponibilidade e o não repúdio dos dados ou da informação e são por exemplo os crimes que estão na Lei do Cibercrime, como o acesso ilegítimo, em que há um compromisso do sistema informático ou a sabotagem, quando os ficheiros são cifrados e perde-se a sua disponibilidade, a pessoa não consegue ter acesso à sua informação. Estes últimos não são do âmbito da nossa atuação, contudo, por vezes, chegam ao nosso conhecimento à mesma, nós fazemos como fazemos com todos os crimes que não são da nossa competência, encaminhamos para o Ministério Público e para o OPC competente.

No Núcleo de cibercriminalidade, quando foi implementado, foram definidos os objetivos, ou seja, dar apoio a toda a estrutura de IC no âmbito da prevenção, deteção e investigação deste tipo de crimes. Nós tínhamos objetivos a curto prazo, para o primeiro ano de existência do núcleo, a médio e a longo prazo. A curto prazo, tínhamos principalmente duas grandes preocupações: formar o próprio efetivo do núcleo (dar formação contínua e uniformizar conhecimentos e procedimentos) e começar a dar apoio o mais rapidamente possível à estrutura de IC, porque comparados com as Polícias dos países vizinhos, nós estamos com muitos anos de atraso no âmbito da investigação da cibercriminalidade. Em termos de atividade operacional, neste primeiro ano, em 2021, apoiámos 53 inquéritos criminais, alguns deles mais como um pedido de apoio, ou com pedidos adicionais de informação, por exemplo, quando surgem novos dados; apoiámos em 54 pedidos de recolha de informação, por exemplo, identificação de suspeitos nas redes sociais, identificação dos IP's, dos seus utilizadores, das mensagens de correio eletrónico. A maior parte dos pedidos diz respeito a burlas. Damos também algum apoio a entidades externas. A médio prazo tínhamos também duas preocupações, que acabámos por começar logo a implementar desde início, porque percebemos com o avançar do trabalho, que eram uma prioridade: a monitorização de fontes abertas (suspeitos em redes sociais, fóruns, troca de informação na *dark web*) e também a realização quer de alertas operacionais para o público interno, para os nossos polícias, quer de ações de esclarecimento para o público externo, para a população em geral e órgãos de comunicação social. Desde o início percebemos que a principal forma de se prevenir a cibercriminalidade e combatê-la é o esclarecimento da população, porque é muito difícil chegar aos autores dos crimes por constrangimentos diversos e legais. Muita da prevenção e do combate que se tem de fazer tem de ser através do esclarecimento e consciencialização das pessoas para a utilização segura da *internet*. A própria pessoa tem de ser o seu principal agente de proteção e de segurança de si próprio. Se conseguirmos mentalizar as pessoas para isso, consegue-se reduzir se calhar um bocadinho da cibercriminalidade. A longo prazo temos como objetivo a especialização por áreas. Neste momento não conseguimos ainda porque a equipa é pequena (1 oficial, 1 chefe e 3 agentes), mas a longo prazo o objetivo é haver uma especialização por áreas: na parte da investigação propriamente dita, na parte da monitorização das redes sociais e a vertente da prevenção e sensibilização da população.

Os crimes tradicionais transformaram-se numa nova modalidade de crime, ou seja, houve quase uma evolução do crime tradicional, porque os crimes já existiam, nós já os investigávamos, só que agora são praticados com outros meios, porque são mais favoráveis aos criminosos, porque correm muito menos riscos. Antigamente nós tínhamos três espaços tradicionais de conflito: terra, mar e ar, e as pessoas sabiam o que acontecia em cada espaço e como é que se movem e que ferramentas utilizam e as pessoas nesses espaços

movem-se fisicamente, têm uma cara e uma identidade. No ciberespaço não, existem diversas ferramentas à disposição do cibercriminoso que lhe permite tanto ocultar a identidade, como mascarar a própria identidade e localização e acaba por ser um ambiente muito mais favorável ao cometimento do crime porque a pessoa não se expõe tanto, não corre tantos riscos, o custo-benefício é claramente favorável ao mesmo. O benefício de conseguir atingir os objetivos e a probabilidade de os conseguir é grande e o risco que corre é mínimo, é muito mais reduzido do que no espaço físico.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: Nós temos de ter ferramentas para trabalhar. Não basta só os conhecimentos teóricos, saber mexer em computadores, etc., é preciso ter algumas ferramentas de *hardware* e *software* que permitam auxiliar as pesquisas. Porque os criminosos também se socorrem dessas ferramentas e têm acesso a elas e utilizam algumas que não são lícitas. Elas têm que existir pois estamos a falar de um espaço que é demasiado complexo e nós não nos podemos socorrer só dos conhecimentos teóricos para atuar. É preciso tanto *know-how* como são precisos equipamentos e ferramentas. Também é preciso um grande trabalho em rede, às vezes falta um bocado de sensibilidade nessa área, porque é preciso compreender que não basta só o trabalho da Polícia, não basta só as Polícias colaborarem entre si, o que já começa a acontecer nesta área do cibercrime, porque já se percebeu que é um crime que não tem fronteiras e não obedece a competências territoriais, nem sequer a barreiras entre países; é preciso também fazer parcerias com o setor privado, com o mundo académico e com o mundo científico, porque são eles que têm o *know-how,* são eles que têm os profissionais qualificados e também são eles que desenvolvem equipamentos e ferramentas. A PSP não tem capacidade para ter esses mesmos profissionais. Nós somos polícias, não somos engenheiros informáticos e também não temos capacidade económica para adquirir ferramentas que são caras e para as desenvolver porque também não temos esse tipo de conhecimentos. Temos de nos socorrer do setor privado e do mundo académico que têm esses conhecimentos e tentar criar parceiras, como já existem noutras Polícias, que nos auxiliem nesta matéria. Isto já acontece em Espanha e em França. Eles próprios dizem que a grande aposta deles é nas parcerias com o setor privado porque são eles que têm o conhecimento e que podem auxiliar.

3. Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: O patrulhamento do ciberespaço, que nós chamamos de monitorização, víamos isso como um objetivo a médio prazo, mas transformou-se num objetivo a curto prazo. Porque tem a ver exatamente com a forma como os processos se vão desenrolando e com o tipo de processos que nós vamos apanhando e com a realidade atual. Nós fazemos alguma monitorização no *nciber*, mas há outros serviços da Polícia que também o fazem, nomeadamente das redes sociais e de alguns fóruns e monitorização de suspeitos. Em certas situações, quando existe um processo concreto ou um suspeito em concreto, faz-se a monitorização desse suspeito, noutros casos monitoriza-se um fenómeno, alguma situação que tenha interesse. No entanto, não temos ainda a capacidade de outras Polícias, em que a monitorização das redes sociais é feita exclusivamente por equipas que só se dedicam a isso, porque isso exige um empenhamento constante. Se estás a fazer um trabalho de patrulhamento, tu não patrulhas hoje fóruns de vendas de armas e amanhã vais monitorizar fóruns de venda de estupefaciente, isso não pode funcionar assim. A pessoa tem de estar dedicada a uma área porque requer que ela conheça o meio em que está a patrulhar, que conheça a linguagem utilizada, que conheça os fóruns, que conheça os grupos mais ou menos que lá atuam e isso exige um trabalho constante. Nós ainda não temos essa capacidade em termos de RH para o fazer. Fazemo-lo em alguns processos concretos e às vezes com suspeitos concretos fazemos essa monitorização, do alvo, da pessoa ou do fenómeno. É um trabalho que a longo prazo e crescendo a equipa, tem que ser feito. Atualmente tudo acontece pela *internet*, mesmo o tráfico de armas ou de estupefaciente, as comunicações são todas feitas através da *internet*, em fóruns privados, pelo whatsApp ou outras plataformas e é a essa realidade que nós nos temos de adaptar.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R: Não, não deve, o ciberespaço é um espaço totalmente diferente dos espaços tradicionais de conflito (terra, mar e ar). Nós agora temos um espaço que não obedece a fronteiras, em que as pessoas têm a capacidade de se anonimizar ou mascarar a sua identidade, onde a informação circula rapidamente em grandes quantidades e é volátil. As ferramentas que os cibercriminosos têm à disposição também são diferentes daquelas que um criminoso tradicional utiliza. A forma de atuar no ciberespaço também não pode ser a mesma de atuar para os

crimes tradicionais, se bem que também não nos podemos esquecer que todo o cibercriminoso tem uma identidade, é uma pessoa. E as pessoas, apesar de atuarem no ciberespaço, também cometem os seus erros depois no mundo terreno. Acaba por ter que haver aqui um bocado de conhecimento das duas áreas, a investigação tradicional continua a ser importante, mas temos que adaptar as ferramentas e os métodos ao espaço que estamos a trabalhar, assim como o tipo de prova que é recolhida, neste caso prova digital.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: Não entendo que seja necessário andarmos a controlar o que as pessoas fazem na *internet*, o que eu defendo é que temos de ter a capacidade de conseguir identificar as pessoas que cometem crimes. As pessoas são livres de utilizar os meios que têm à sua disposição e de utilizarem a *internet* livremente, cada um deve ser responsável e utilizá-la de forma consciente, para evitar expor-se a riscos. O que nós temos de ter capacidade é, além de tentar prevenir, desenvolver campanhas, sensibilizar as pessoas para a utilização consciente da *internet*, e quando acontece um crime, nós termos mecanismos que nos permitam identificar os suspeitos. Não esbarremos em obstáculos legislativos que não permitem avançar e chegar àquela identificação. Um exemplo concreto são as burlas *online*, em que nós vamos identificar o cabeçalho técnico da mensagem de correio eletrónico do *email* e o IP do computador vai ter aos Estados Unidos, à Rússia e China, nós identificamos qual é a operadora que está a fornecer o serviço, depois tem de ser feito o pedido para que ela forneça os dados do utilizador. Qual é a obrigatoriedade dessa operadora responder a um pedido de Portugal? Mas o crime foi cometido e existe uma ou várias vítimas. Este controlo sim, tem de haver mecanismos legais que obriguem a que as operadoras, além de terem de verificar os dados de quem se regista, que é um outro problema: a forma como os registos são feitos em plataformas, a pessoa fornece os dados que quiser, ninguém vai verificar se os dados são reais ou não, em algumas plataformas basta um nome e endereço de correio eletrónico, sem qualquer dado de identificação fidedigno, que permita em caso de necessidade, identificar aquele utilizador; e ainda deveria existir uma obrigatoriedade de, perante um crime, a operadora ser responsável e ter de fornecer os dados de quem tem registado e de quem está identificado com aquele IP.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: As equipas de proximidade da PSP fazem um excelente trabalho. Nesta vertente do cibercrime eles têm feito algum trabalho na questão do ciber*bullying* por exemplo, nas escolas e mesmo esclarecimentos sobre a *internet* segura, etc. Eles devem continuar a fazê-lo. Mas não basta trabalhar com as crianças, a vítima de cibercriminalidade pode ser qualquer pessoa, com qualquer idade, nós já apanhámos de tudo: situações com menores de idade, com adultos de várias idades e de ambos os sexos e diferentes graus de escolaridade. Qualquer pessoa pode vir a ser vítima. A atuação das equipas de proximidade nesta área tem de ser mais abrangente. Junto das crianças, claro que tem de existir uma sensibilização relativamente à forma como elas utilizam a *internet* e os riscos que correm, porque as crianças não se podem esquecer que o que lá colocam fica lá para sempre. Também tem de existir uma sensibilização dos pais porque têm de perceber com quem é que os seus filhos se relacionam e a quem "abrem a porta", o que partilham e o que fazem quando utilizam a *internet* e as redes sociais. Tem de haver uma educação por parte dos professores também, para que consigam identificar sinais de alerta. E ainda uma consciencialização não só focada na vítima mas também na dissuasão dos potenciais criminosos. Isto aqui pode ser feito nas idades mais jovens, por exemplo agora estamos a participar num projeto europeu, muito interessante porque tem uma perspetiva diferente. Normalmente os projetos de prevenção focam-se na vítima e em consciencializar a pessoa sobre os riscos que corre e sobre as medidas de autoproteção, este projeto foca-se na dissuasão do potencial cibercriminoso enveredar por caminhos ilícitos. É aplicado aos mais jovens, porque quando estamos a falar de cibercriminalidade e da dissuasão de potenciais criminosos estamos a falar em idades ainda precoces, se estivermos a falar de idades adultas, isto já não vai funcionar porque a pessoa já sabe o que é e o que pratica. Estamos a falar é daqueles jovens que começam a ter interesse na área, a ter curiosidade e a fazer pesquisas na *internet* de como *hackear* um jogo, por exemplo. Portanto os jovens fazem uma pesquisa na *net* sobre *hacking* ou sobre *RAT* e vai-lhes aparecer uma mensagem/um alerta a dizer "atenção que o *hacking*, o *RAT* é crime", depois tem um *link*, que é um *website* e dentro deste tem lá a descrição do tipo de crime em que ele está a incorrer, as consequências penais e consequências para o seu futuro, em termos de registo criminal, de entrada no mercado de trabalho, etc. Por outro lado, também lhe oferece caminhos alternativos, com informação sobre cursos profissionais ou superiores que pode tirar nessa área ou fóruns de partilha de informação nessa área lícitos, clubes de codificação, entre outros.

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: Sinceramente em todo o público-alvo. Dependendo do tipo de crime que estejamos a falar, existe um público-alvo que prevalece. Em termos da dissuasão, nos termos que expliquei aplica-se sobretudo aos mais novos. Depois a consciencialização para a utilização segura da *internet* e para os riscos que correm, tem de ser feita em várias idades, porque se falarmos das burlas informáticas, das falsas vendas, que é das tipologias que mais tem crescido nos últimos tempos, principalmente com a pandemia, porque as pessoas passaram a comprar muito mais de forma *online*, mesmo quem nunca o tinha feito, viu-se "obrigado"/ na contingência de ter que o fazer, algumas pessoas não estavam familiarizadas com este mecanismo não tinham consciência dos riscos que existem e por isso eram muito mais suscetíveis a serem enganadas. Este público-alvo também tem de ser consciencializado, como também é importante ser consciencializado o público mais idoso, que é muitas vezes vítima de burla. Temos o exemplo do fenómeno das burlas amorosas/esquemas românticos que atinge muito esta população. Com a pandemia algumas pessoas ficaram ainda mais isoladas, porque deixaram de poder frequentar alguns espaços de convívio e pessoas que nunca tiveram redes sociais, começaram a utilizar o *facebook*, começam a adicionar "amigos", a estabelecer contactos e estamos a falar por vezes de pessoas que estão numa idade mais avançada e se sentem sozinhas, porque já não têm os filhos em casa, que estão emocionalmente vulneráveis e mais suscetíveis de serem alvo deste tipo de burla.
Mas qualquer pessoa, em qualquer faixa etária e de qualquer sexo, pode ser vítima de cibercrime. Existem certas tipologias de cibercrime que atinge um alvo mais específico: se falamos dos predadores *online*, são os mais jovens e crianças; se falarmos das burlas, estamos a falar de qualquer faixa etária porque toda a gente compra *online*; a questão das burlas amorosas acontece muito com faixas etárias de meia-idade (por exemplo pessoas divorciadas, que já tiveram uma primeira relação falhada e agora querem acertar, porque estão numa idade em que começam a ter receio de envelhecer sozinhas) e mais elevadas. Tem que haver uma informação constante para as pessoas, campanhas, alertas, tem que se apostar na comunicação social para a consciencialização das pessoas (divulgar determinados fenómenos que são detetados para dar a conhecer às pessoas). Em relação às falsas vendas, muitas vezes os próprios *sites* têm indicadores, a pessoa se estiver com atenção em averiguar se a fonte é fidedigna, antes de comprar, facilmente identifica alguns aspetos que causam desconfiança. Normalmente o *link* do *site* real e o *link* do *site* falso são muito semelhantes, as primeiras letras até costumam ser iguais à marca que estão a imitar, mas depois a terminação é diferente e é uma terminação que não é habitual de se ver num *site* oficial. É preciso ter atenção a esses pormenores. Se a pessoa vai com o impulso de querer comprar porque o preço é bom, é muitas vezes levada ao engano. Foi o que aconteceu com a marca *stradivarius*, nós depois fizemos uma campanha com o *print* de alguns *sites* fraudulentos, identificando os pontos no *site* que mostravam que o *site* não era fidedigno. Por vezes também são utilizados tradutores automáticos para a construção dos *sites* e é possível observar uma ou outra palavra mal traduzida, num português mal escrito. Por exemplo, vemos muitas vezes a palavra "*help*" literalmente traduzida para "socorro" nesses *sites* fraudulentos.

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: Os riscos são muitos, principalmente a questão dos predadores *online*, porque as crianças não têm consciência dos riscos que correm, não estão alertadas para estas questões. Mesmo com os próprios pares, quando nós falamos, e acontece com a questão do ciber*bullying,* os jovens pensam que é só uma brincadeira, "vou só pôr aqui uma fotografia do X, para fazer rir os colegas" e não é uma brincadeira, é um crime e tem consequências para o visado. É esta consciencialização que é precisa, pelos pais e professores e que as equipas de proximidade também podem fazer. As crianças por vezes não têm consciência dos atos que cometem e não sabem que estes configuram crimes, com consequências para os pares, nem dos riscos a que se expõem quando partilham determinadas informações pessoais ou quando adicionam um "amigo" que não conhecem, pensam que é da mesma idade porque partilha os mesmos gostos e do outro lado pode ser um predador. Tem de passar muito pela educação. Mesmo havendo um patrulhamento da Polícia na *internet* destinado a identificar predadores sexuais, é impossível prevenir se a própria pessoa se expuser aos riscos. Não há um polícia para cada criança, para cada utilizador da *internet*. A utilização segura tem de passar pela educação.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: Desafios é o que não falta. Para além do que já temos hoje, no cibercrime e no ciberespaço recorre-se de ferramentas que estão em constante mutação. A tecnologia está em constante evolução, e ela é boa quando fazemos uma boa utilização mas a evolução também favorece quem faz uma má utilização. Se a tecnologia evolui, os cibercriminosos também, não falamos só de um criminoso que comete um ilícito a partir de casa, mas falando de grupos organizados, que há, as tecnologias favorecem estas pessoas, que lucram bastante com estes crimes *online*, que têm capacidade económica para investir em tecnologia diversa que mascara a sua identificação e localização e a Polícia não tem tanta capacidade económica para adquirir ferramentas que permitam competir com essa capacidade. Estamos a falar de um mundo em que as coisas estão sempre a evoluir e nós não temos capacidade para acompanhar. Além disso, existem outros desafios que vão ser colocados, que

têm a ver com a evolução da própria sociedade e com esta vivência e necessidade que temos de comunicar através das redes sociais e estar constantemente a viver a nossa vida *online*, porque queremos ter acesso a tudo no preciso instante em que precisamos das coisas. A *internet* das coisas, as pessoas querem estar fora de casa e ter acesso e controlar tudo no seu interior, e esta conexão de tudo com tudo também acaba por nos colocar desafios. Quando falamos deste nível de conexão, não falamos só das nossas casas, mesmo a própria cidade, o mundo, está-se a organizar dessa forma. E agora nós vimos que quando ocorre um ataque, se acontecer na nossa casa a vítima somos apenas nós, mas se for numa infraestrutura crítica (sistema da segurança social, fornecimento de água, energia ou *internet*), afeta a população em geral. Como aconteceu agora com a Vodafone, vemos quais são as implicações que isso tem. Porque é bom, realmente, nós termos acesso a tudo em tempo imediato mas quantas mais ligações nós temos, mais suscetíveis estamos, havendo um ataque, se eu tiver vários equipamentos ligados, fico sem acesso a todos. A evolução tecnológica facilita muito a nossa vida mas também nos pode causar sérios constrangimentos, quando ocorre um ataque as consequências são muito mais devastadoras do que eram antigamente, e com a utilização do 5G pior ainda. Porque vem aumentar a velocidade da comunicação, vem permitir que a *internet* das coisas possibilite a conexão de muitos mais equipamentos em simultâneo e com as consequências que podem advir daí. A alternativa é investir na segurança, na segurança de redes e infraestruturas, na segurança humana e na criação de planos de contingência. Mais do que uma preocupação, a questão da implementação de medidas de segurança tem que começar a ser encarada como um dever pelas organizações.

Informador qualificado 3

Cargo: Subintendente, Chefe do Núcleo de Apoio Operacional do DIC

Data: 11 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: Na prevenção há sempre dois pilares importantes: as políticas e a divulgação a nível do policiamento de primeira linha. Começar pelas escolas, que penso que o que funciona melhor em termos de prevenção é o policiamento de proximidade, divulgar também nas redes sociais, que já tem sido feito, para as pessoas terem alguns cuidados. Se bem que tenho muitas dúvidas que isso funcione efetivamente. As pessoas vão começar a ter mais cuidados quando sentirem na pele que há riscos e que há coisas que devem acautelar. A nível de prevenção, ela entra aí, gerar um contexto de cuidados a ter e de políticas de intervenção, etc. Depois, ainda na prevenção, é o ciberpatrulhamento a funcionar, que na PSP já começa a existir, ainda que de uma forma ainda rudimentar, para antever situações que possam vir a acontecer em termos criminais. Isto no domínio da prevenção, porque investigar também é prevenir. No domínio do combate, é sinalizar as situações e investigá-las devidamente, com meios, com tecnologia, com recursos humanos, e isso é um caminho que ainda não está a ser feito. Se fizermos aqui um paralelo com a construção, já está lançada a primeira pedra, mas a Polícia está muito longe mas mesmo muito de ter uma estrutura eficaz no combate ao cibercrime.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: Essa é uma responsabilidade que não é só da PSP, aliás a responsabilidade da PSP nesse domínio não é consensual, embora tenhamos alguns crimes praticados por ambiente digital em que a investigação recai sobre a PSP. Temos tido até alguns casos de algum sucesso. Tivemos recentemente alguns processos-crime a nível nacional, o "brandfurt" foi uma investigação muito grande a nível nacional, embora depois em julgamento tenha caído a prova quase toda, mas eliminou-se o foco do crime, que eram burlas através do OLX. Apesar de isto não estar bem conotado com cibercrime, porque o cibercrime é mesmo a intervenção junto dos equipamentos digitais, a manipulação e eventualmente depois a extorsão para pedir resgates, etc. Portanto são coisas um bocado diferentes. Mas se nós quisermos chamar cibercrime a tudo o que passa por via de um computador, então isto poderá entrar aqui nesta discussão. Como reforçar: é a sinalização, recursos humanos devidamente formados que não há, meios técnicos especiais de investigação criminal nestes casos que também não há, mas tudo vai começar sempre pela sinalização. Essa sinalização já vai sendo feita, ao nível do departamento passa pelo núcleo de análise e também pelo núcleo de cibercriminalidade. E depois tem de ser consequente, ou seja, tem de haver investigações de facto com meios e isso não existe. A PSP não está ainda preparada para esta realidade. Portanto o que temos de fazer se calhar é começar a casa pelo início, é perceber onde queremos chegar, que recursos é que precisamos (recursos humanos naturalmente, meios materiais) e

começar a tratar disso debaixo para cima, começar os pilares até ao telhado, não começar a casa a meio.

3. Como se adaptou/adapta o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: O patrulhamento do ciberespaço já existe há muitos anos noutros países e cá em Portugal também já há uns anos. Portanto vamos necessitar de pessoas devidamente formadas e que a tempo inteiro naveguem na *dark web* ou na *internet* dita comum e sinalizem situações de potencial prática criminal. O que nós temos de ter na PSP, se o queremos fazer, é ter pessoas formadas que, num determinado local, têm objetivos concretos e apenas fazem isso para sinalizar situações. Agora eles sinalizam e eventualmente poderão ali fazer algumas diligências prévias de investigação, portanto tentar perceber ali um bocadinho mais, mas depois a competência deles cessa ali, tem de ser comunicado, o MP tem de autuar o inquérito e depois aquilo tem de ser distribuído, etc. Mas o patrulhamento faz-se assim, faz-se na sinalização deste tipo de situações, na introdução de operacionais nossos na *dark net* e na *web* dita comum para sinalizar estes casos. É assim que se faz. Agora, isto não se faz sentando uma pessoa numa secretária num computador ligado à RNSI atenção. Eu acho que o problema principal e atual na PSP é que a generalidade das pessoas e até algumas pessoas que acabam por decidir talvez não estejam devidamente informadas disso. É impraticável fazer patrulhamento com um computador todo ligado à rede comum porque qualquer indivíduo que anda na *dark net* tem conhecimentos mínimos de informática e vai detetar os IP´s, vai detetar a localização, isto não se faz assim. E a PSP, não está preparada em termos logísticos para este tipo de funções, portanto temos de nos preparar, adaptar. Um "patrulheiro" digital não se pode conectar à *internet* com um cartão cujo pagamento é identificável que é a PSP que o paga, por exemplo. Nós não temos mecanismos para chegar ali ao multibanco e carregar um cartão pré-pago para nos conectarmos à *internet*. Isso não existe. Não há previsão legal para fazer esse tipo de despesa, portanto isto são questões que não são novas, mas que ainda não têm resolução. Isto é o domínio logístico. No domínio da ação propriamente dita, um "patrulheiro" no ambiente digital, vai ter de criar uma história de cobertura, vai ter de criar ali um, que no momento chamam de avatar, vai ter de criar uma personagem e isso não se faz em dois dias, isso alimenta-se, às vezes durante meses ou anos. Tem de haver este conhecimento e essa predisposição. Se nós iniciarmos hoje um processo desses, ele vai surtir efeitos se calhar daqui a um ano, a um ano e meio. É todo esse conjunto de *handicaps* que nós temos ainda que acho que ainda não ultrapassámos.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R: Há particularidades, claro que sim. Há especificidades muito concretas no cibercrime, como há noutro tipo de investigações. A investigação criminal é pluridisciplinar, é uma das suas características e neste caso aqui, tem particularidades distintas das outras. Quem quiser fazer patrulhamento e até investigação destes casos, tem de ter equipamentos, tem de ter uma estrutura criada, que ainda não existe. Nesse aspeto é completamente diferente de investigarmos outro tipo de criminalidade. Mas isso é transversal à IC. Investigar droga é diferente de investigar furtos, roubos, criminalidade económico-financeira, etc.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: Essa é a grande questão que se coloca em tudo o que é IC: até onde é que está o limite entre aquilo que são os deveres da investigação e os Direitos Fundamentais das pessoas. Isso é muito difícil de balancear, não é só aqui na questão do cibercrime e do controlo *online*, mas é em tudo. É uma questão longa, que exige muito tempo. Bem isso, eu acho que vai sempre depender das repercussões que o crime tem e a Lei prevê isso, não há aqui nada para a qual a Lei não tenha previsão. Tem que haver proporcionalidade e adequação nos meios. Às vezes a medida pode até não ser proporcional, ou seja, exagerada por parte das Polícias e demasiado ofensiva aos Direitos Fundamentais, mas se não há outra forma, nenhuma forma de lá chegar que não seja por aí, então terá que ser assim. Por exemplo, funciona um pouco como as escutas telefónicas, que nos anos 90 e na primeira década e na década de 2000 tiveram o seu auge, hoje estão em decadência por outros motivos, mas colocava-se muito essa questão, principalmente nos anos 90, que eram demasiado ofensivas e intrusivas na esfera da liberdade das pessoas, porque ouvia as conversas que tinham, de conteúdo íntimo, etc. Mas, aliás para um juiz autorizar uma interceção telefónica, tem de ficar taxativamente fundamentado que não havia outra forma de chegar à prova que não seja pelas escutas telefónicas. Acho que é o mesmo que se vai aplicar aqui no cibercrime. Imaginando, a lei já começa a prever algumas formas de introdução de *malware* mais ou menos, há assim umas coisas um bocado estranhas, mas se tivermos que ir para aí, para introduzir um *malware* num equipamento, telemóvel, computador, se não há outra forma de chegar à prova, isso vai ter de ser aceite. Portanto aí, e é claro que isso é altamente intrusivo, porque a partir do momento em que se introduz o *malware* num telefone e conseguimos à distância perceber tudo o que lá está, isso é altamente intrusivo, é muito mais intrusivo do que uma escuta telefónica, sem dúvida alguma. Mas caminhamos para aí. No entanto, também do

outro lado, é altamente intrusivo que um *hacker*, num lado qualquer me introduza a mim um *malware* e saiba tudo o que eu tenho aqui e, para além de saber, exerça uma extorsão sobre mim. Portanto, aqui é a adequação do meio e a proporcionalidade, mas tem que se ir medindo, é claro que não se vai introduzir um *malware* para captar toda a informação a um telefone a quem está a fazer uma burla ou ameaças que não tenham grande relevância, eu penso que não é proporcional, mas é um juízo que tem de ser feito pelo MP.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: Eu não acredito que, no âmbito do MIPP se vá conseguir trabalhar este tipo de questões, a não ser eventualmente na difusão de comportamentos que sejam preventivos: mudar as *passwords*, não ter a mesma para tudo, ter *passwords* difíceis, essas coisas assim mais simples e há outras. Mas ao nível do MIPP e daquilo que é hoje o MIPP, não vejo outro tipo de mais-valia que não esta difusão. Mas essa difusão tem de ser feita também de forma generalizada, porque não é o MIPP passar e contactar com determinadas pessoas "o senhor não se esqueça de criar *passwords* complexas...", ninguém vai ligar a nada disso. Agora, ações de sensibilização para um número elevado de pessoas nas escolas, nas faculdades, e assim. Aí eu penso que poderá ter algum efeito, mas o principal não é por aí, não vai ser por aí, o principal é nós termos uma estrutura de investigação criminal célere e eficaz. A estrutura deve estar na repressão. A prevenção também é muito difícil de medir, mas penso que não será por aí.

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: O público-alvo deve começar nas crianças e jovens e eu vejo isso, eu tenho filhos e percebo que há perigos e que eles não estão devidamente sensibilizados para algumas questões. Tenho um filho com 12 anos que acede ao *youtube*, publica vídeos dele, porque ele faz filmes e canta e isso entra ali nalguns perigos. Por isso deve-se começar por estes, até porque acho que é o único caminho ainda que o MIPP poderá ter de chegar de forma generalizada. É chegar a um auditório de uma escola secundária ou escola básica, porque mais novos do que isso, não me parece que vão perceber grande coisa e explicar-lhes, ter uma apresentação, um filme, algo que lhes elucide dos problemas que podem advir desta questão. Agora, isto nem sempre é cibercrime, o cibercrime puro e duro não é bem isto. Isto são crimes praticados pelo meio digital, são coisas ligeiramente diferentes. Mas ao nível do MIPP é o que eu acho que pode ser feito.

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: Crianças em particular podem ser vítimas de crime de extorsão. Navegam na *internet*, são inocentes, pensam que tudo o que publicarem só os amigos é que vão ver e que não há perigo nenhum. Eles não têm a medida do perigo, se vão atravessar uma estrada sabem que o carro pode vir e tem perigo, na *internet* é tudo invisível, não há medida do perigo e nesse sentido, postam filmes, fotografias, a sua localização… Pode haver aqui depois a questão dos crimes sexuais, a pedofilia, raptos, violações, etc. Isso é um número reduzido mas é um perigo que existe. Fundamentalmente é a questão da extorsão, de alguém aceder, saber onde ele está e depois tentar aqui questões de extorsão. Mas também há o perigo físico dos crimes sexuais e por aí. Não tem muita dimensão em Portugal, daquilo que sabemos, dos números, mas obviamente que é um perigo, mas lá está, nós não vivemos numa bolha e com isto do *covid* e dos confinamentos, aumentou também a utilização destes meios, porque as crianças deixaram de brincar, de ter outro tipo de contactos. É um perigo é, mas não me parece que seja preocupante.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: No futuro não sei muito bem, sei que no presente nós já temos alguns problemas. Aliás esta semana foi pródiga em relevar alguns desses problemas. Porque a verdade, ou aquilo que nós achamos que seja a verdade, é que não há em Portugal uma cultura de defesa a nível de cibercriminalidade. O choque tecnológico nunca se fez em Portugal e nas Polícias então é que não se fez mesmo. Porque houve algumas empresas em Portugal que fizeram alguma parte do choque tecnológico, principalmente aquelas de dinâmica internacional mas este choque na Administração Pública nunca existiu. O que existiu foi comprarem computadores. A preparação para a tecnologia não existe e nas Polícias também não existe. A PJ está um pouco melhor, mas também não existe o choque tecnológico. Uma boa parte (isto é uma coisa que devia ser estudada) dos Polícias são infoexcluídos e da hierarquia dos polícias são infoexcluídos e não sabem o que é um servidor sequer. Isto é um desafio, é preparar os recursos humanos para lidar com este tipo de situações. Arrisco-me a dizer que mais de metade do efetivo da Polícia é infoexcluído, sabe aceder a um computador claro que sim, mas perceber minimamente como as coisas funcionam, não percebe e eu acho que esse é o maior desafio. Porque nós podemos comprar material e equipamento, é relativamente simples, vem o Orçamento de Estado e alguém tem uma ideia, alguém

assina e compra-se, o problema depois é criar uma estrutura que funcione. Isso é que é o desafio, montar uma estrutura é algo muito difícil. E eu acho que o maior desafio, a nível da PSP, será preparar os recursos humanos e montar uma estrutura eficaz e isso vai ser muito difícil, vai ser um grande desafio, mas conto também que estes trabalhos abram pelo menos a discussão para o que se deve fazer.

Informador qualificado 4

Cargo: Intendente, autor de vários artigos sobre cibersegurança

Data: 1 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: Nós começámos dia 1 (de fevereiro) uma campanha, neste momento está a decorrer uma campanha até dia 9, porque é o Dia da *Internet* mais Segura. E é justamente neste âmbito que a PSP se deve circunscrever mais, que é no campo da prevenção. E é normalmente aí que nós temos trabalhado muito, mas a verdade é também que, desde logo se se ler a LOIC, é possível, à luz daquilo que é a pequena complexidade dos crimes, o Ministério Público delegar a competência de crimes que normalmente são da competência da PJ, noutras Forças de Segurança. E pelos vistos é isso que está a acontecer. Pessoalmente, quando trabalhei na parte operacional, tudo o que tinha a ver com o cibercrime, ainda que o computador fosse utilizado apenas como um instrumento para atingir um fim, por exemplo no caso da violência doméstica, nós remetíamos à PJ. Aquilo que eu sei é que neste momento a PSP está, por exemplo no caso da VD, em que publicar fotos para atingir determinada pessoa, um ex-parceiro ou ex-parceira é enquadrável também no crime de VD, a desenvolver este tipo de inquéritos. E pelos vistos, neste momento também já vamos tendo alguma capacidade técnica, no Núcleo de Cibercriminalidade, que está a receber vários pedidos, quer nossos, quer do MP. Ou seja, a minha convicção, justamente pela minha experiência profissional, foi de que nós PSP, não devíamos entrar por aquilo que é a investigação criminal nesta área, justamente porque achava, essa era a minha realidade, porque não tínhamos capacidade técnica nem legal para assumir esse tipo de processos-crime, salvo quando a tal complexidade, a tal exceção de o MP poder delegar noutros OPC crimes que são da competência de um determinado OPC, que é o caso da PJ. No entanto, a PSP neste momento, está a receber muitas solicitações nesse sentido.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: Eu estou muito convicto que o nosso papel, quer da PSP, quer da GNR, porque acho que ainda estamos a percorrer um caminho que é muito embrionário em termos de investigação do ciberespaço, é a prevenção. Podemos fazer muito na área da prevenção, porque temos uma malha com uma dispersão geográfica enorme, podemos chegar a milhares de alunos, a milhares de pais, a milhares de idosos, e aí assim acredito que podemos fazer um excelente papel e fazemo-lo. Aliás a Direção Nacional, todos os anos, impõe objetivos nacionais, distritais e dentro desses objetivos há números que surgem no âmbito daquilo que são ações de sensibilização nas mais diversas áreas (violência doméstica, *bullying*, etc.), uma delas há-de ser ao nível daquilo que é a prevenção por exemplo do ciber*bullying* ou da violência no namoro no âmbito das redes sociais. Agora o que se pode fazer mais? Bem, se pensarmos que provavelmente a PSP está a ganhar cada vez mais espaço na investigação deste tipo de crimes, então o que provavelmente temos de fazer mais é reforçar as competências dos nossos homens que trabalham na estrutura da IC, ao nível da formação e em termos técnicos. Neste momento não tenho conhecimento de os Comandos estarem apetrechados de equipamentos, tirando esta realidade que está centralizada no DIC e que dizem que é um gabinete que está muito bem equipado e que tanto assim é que tem recebido cada vez mais pedidos externos.
Só vejo neste quadro de reforçar a formação. No quinto curso de IC, em 2002, não se falava na altura em cibercrime, nem cibersegurança nem em ações de sensibilização, portanto isto é algo muito recente para nós, PSP. Hoje, em 2022, o cenário estará diferente, porque o que me tem chegado, é que o MP já vai delegando também na PSP e provavelmente na GNR a investigação deste tipo de crimes, quando a complexidade não é grande.

3. Como se adaptou/adapta o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: Eu não diria que neste momento nós fazemos um patrulhamento do ciberespaço, o que nós fazemos é trabalhar a fase pré-crime, isso sim fazemos muito e fazemos bem. Os elementos do MIPP, das EPES têm a vida muito ocupada, depois até há dificuldades com as Direções das Escolas, porque eles quase que impõem, têm objetivos para cumprir de ações de sensibilização mas as escolas têm de arranjar horários específicos para os polícias irem lá e falar. Se na PSP existe ciberpoliciamento? Eventualmente existe, mas direcionado para aquilo que é o trabalho das informações, e aí sim sabemos que há polícias que o seu dia-a-dia é navegar no ciberespaço para sinalizar ou projetar cenários. Quando por exemplo, nas redes sociais, percebemos que há um grupo espontâneo que está a preparar uma manifestação no Marquês de Pombal. Podemos falar de ciberpoliciamento, na ótica de prever comportamentos e cenários. Nessa perspetiva de prevenção, podemos falar no ciberpoliciamento mas ligado nesta ótica das informações, ou seja, recolher informação para melhor decidir no terreno, apoiar a decisão no terreno, informando desde logo quem comanda que "à partida, no dia 24 de janeiro vai haver uma concentração à frente da Assembleia da República, porque temos estas evidências". Não propriamente com o efeito que nós falamos do policiamento tradicional, da visibilidade policial e em função da visibilidade policial haver aqui um efeito de retração das pessoas. Ou seja, haver alguém que está a pensar cometer um crime e sente a presença da PSP, isso não acontece. Haver esse efeito dissuasor por parte da PSP junto de potenciais criminosos ou então a PSP surgir como o tal guardião, em que se fala na Teoria das Atividades Rotineiras, na fórmula do crime, em que um dos fatores para que ocorra crime é a ausência de guardião. É o que acontece quando alguém pensa que vai cometer um crime na via pública, mas vê uma farda azul ao fundo, retrai-se. Isso não acontecerá no ciberespaço. Pode amanhã acontecer, não sei como tecnicamente, alguém que está a ponderar cometer um crime e sentir a presença da Polícia; haver tipo um alerta. Faz lembrar tal como nós polícias temos graus de acesso à informação no computador de serviço, quem acedesse a um determinado conteúdo que não devia, aparecia um alerta. Havia como que um polícia, um *big brother* sempre presente. Ou então como acontece, por exemplo com quem anda a visitar determinados *sites* que estão a ser monitorizados por parte da PJ, depois mais tarde vir a ser constituído arguido por *sites* de pornografia infantil ou outros. Mas aí já é na perspetiva de sinalizar quem comete crime e depois atuar junto dessa pessoa e não propriamente na ótica como olhamos o policiamento, que é na ótica da prevenção: é visibilidade para prevenir. Visibilidade para reforçar a ideia de que há um guardião, para que quem pondere os prós e contras, entre cometer ou não crime, ser conduzido a não cometer, justamente porque viu uma farda ou sente que a Polícia está presente. Isso pode acontecer se a pessoa que está a ponderar cometer um crime no ciberespaço sentir que de facto a Polícia está mais atenta, ou que a tal procura/busca foi reforçada. Mas para isso tínhamos que vender esta imagem de que a PJ, PSP e GNR está presente, ainda que não a sintamos, ela está presente. Não sei até que ponto é que isso depois também não põe em causa direitos.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R: Continuo a achar que não se pode falar em patrulhamento do ciberespaço, nem se quer consigo imaginar como é que é possível em termos legais. Ao nível das informações, não se pode dizer que é propriamente um ciberpoliciamento, porque o que os nossos polícias das Informações fazem é justamente pesquisar, por exemplo, nas redes sociais, em fontes abertas, não andam propriamente em espaços reservados ou a tentar perceber onde anda alguém, qual é o percurso dessa pessoa, mas não tenho dúvidas que andam em fontes abertas à procura de sinais. Não é o policiamento da forma como conhecemos, é um trabalho de análise. Ou seja, tem um foco que é sinalizar comportamentos desviantes, sem que as pessoas que estão a ser, neste caso, observadas, saibam que isso está a acontecer. Porque na rua, quando um polícia olha para nós, sabemos que estamos a ser observados por ela e restringimo-nos, se queríamos fazer uma coisa menos correta, já não o fazemos, outra coisa é a pessoa ter uma página pessoal no *facebook* e saber que a Polícia está com a sua página aberta. Mas não há nenhum mal, até porque a página é pública e qualquer pessoa pode procurar por ela, a diferença é que a Polícia, quando faz essa análise, o que está à procura, se for um trabalho sério, é sinalizar e prever cenários para apoiar a decisão de quem está a comandar. As informações da PSP estão constantemente a emanar relatórios e o trabalho das informações, mais do que a prevenção, visa sobretudo apoiar a decisão. Este trabalho muitas vezes não vem impedir que ocorra o crime, vem é ajudar quem depois comanda aquela área ter conhecimento prévio para depois atuar. Por exemplo, vai haver uma manifestação de coletes amarelos, as informações recolhem tudo o que têm e não quer dizer que aquilo não vá ocorrer, não há aqui o trabalho que é desenvolvido no policiamento tradicional em que passa um carro patrulha ou um homem fardado e as pessoas deixam de cometer aquele comportamento. Não é isso que acontece. O que acontece é o trabalho de informações para colherem informações para fazer chegar ao decisor e apoiar a sua decisão. A especificidade entre Polícia, neste caso PSP e ciberespaço, é na dimensão da prevenção, não propriamente o trabalho no ciberespaço mas o trabalho com as potenciais vítimas, as crianças, os mais idosos e também esta franja pelos vistos que vamos tendo que é tendencialmente crescente de processos-crime que já vamos recebendo. Onde eu penso que já temos trabalhado muito é ao nível das informações, o nosso Departamento de Informações Policiais não tenho dúvida que trabalha e há muito tempo mas na ótica de apoiar a decisão e de prevenção, em

fontes abertas: lendo nas entrelinhas, todos os dias sai um apanhado de todas as notícias que saem sobre a PSP, que é difundido pelos Comandos, mas não só, juntar sinais que, potencialmente venham dar origem a concentrações, manifestações, etc. Quando se envia um relatório por exemplo aos comandantes a dizer quais são os movimentos dos *Hell Angels*, também é apoiar a decisão, mas quando se apoia a decisão também estamos a ajudar os comandantes a prevenir eventualmente alguns comportamentos desviantes.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: O controlo só faz sentido nesta lógica, que é quando há condutas que estão sinalizadas como ilegais e que conseguimos circunscreve-las quando fazemos essa análise. Esta circunscrição ao comportamento que é crime e a certos repositórios/espaços onde tendencialmente quem os frequenta são pessoas que cometem crime. É claro que quando fazemos essa avaliação, provavelmente vamos encontrar pessoas que não têm culpa, que foram apanhadas na interceção dessa pesquisa. Mas é preciso um certo enquadramento, tudo isto faz sentido desde que o MP esteja a par, é preciso um respaldo da Autoridade Judiciária. O limite deve ser esse: havendo uma atuação policial, com respaldo desde logo legitimado pela Autoridade Judiciária e circunscrita naquilo que são franjas do ciberespaço, um dos melhores exemplos são *sites* de pornografia infantil ou que se venda produtos de pornografia infantil. Tudo o que fuja desses espaços, só porque "vamos estar aqui atentos, porque nunca se sabe o que pode sair dali", não pode ser, porque se não depois estávamos a entrar na discricionariedade, que é o que acontece também na rua. Na rua quando um polícia autua meia dúzia de carros e não autua a outra meia dúzia, é a discricionariedade que entra. "Deixe-me cá ver a aspirante Sara, por onde é que anda", isso deve ser possível chegar lá, qual é a sua pegada digital, quais são os *sites* que consultou. É a devassa da vida privada e é crime. O policiamento à partida, não estamos a falar de mandados de busca nem nada disso, mas no policiamento tradicional não há limites, aliás há quem diga que há zonas em que a Polícia já nem entra, mas na teoria não há limites, a qualquer hora e em qualquer dia, entra em qualquer sítio para policiar a título preventivo, para prevenir comportamentos desviantes. Agora, passar isso para o ciberespaço é que me parece não ser possível.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: Temos o trabalho que é desenvolvido pelas EPES que, neste caso, já há uns anos e sobretudo nos últimos anos quando se começou a falar mais no ciber*bullying* e mesmo a ligação entre a violência no namoro e as redes sociais e isso é algo muito recente. A violência no namoro só em 2013 foi introduzida no art.º 152.º do CP (Violência Doméstica), estamos a falar há 7, 8 anos e é sobretudo na última meia dúzia de anos que a PSP começou a introduzir nos seus conteúdos que ministra nas escolas estas áreas. Que é uma área que a maior parte dos jovens, é como um peixe dentro de água, sentem-se completamente à vontade mas que ainda assim não têm noção exata dos perigos. Tanto é que, quando falamos na tal ausência de guardião, muito disto acontece justamente porque o guardião, neste caso, o pai ou a mãe, não exerce o seu poder de supervisão, de controlo parental. Às vezes questionamos como é que uma criança dá por ela a falar com um predador há meses, convencida que é alguém da idade dela e vai ao seu encontro. Há vários relatos desses. E onde estavam os pais nesse processo? Porque também parece que como a autoridade em geral está em crise em Portugal, os pais também têm algum receio de exercer a sua autoridade, que é uma coisa curiosa. Há aqui uma relação de autoridade que deve ser exercida, não somos todos iguais e quando os pais acham que não são bem pais, são amigos e "tens a tua liberdade e eu fica-me mal controlar a tua liberdade", temos estes problemas. Ou se convertem em pequenos ditadores, ou nem admitem que um pai perceba por onde ele anda a navegar, é a sua esfera pessoal. Mas depois acontecem estas coisas e os pais ficam chocados, magoados e tristes com situações destas, violações, etc. O que se pode fazer mais ao nível das EPES, do MIPP? Neste momento já temos, em quantidades industriais, ações de sensibilização que são feitas ao nível das várias escolas. Posso dar uma boa prática que colhi da Polícia Holandesa, já em 1998, há 24 anos: as escolas tinham uma unidade curricular chamada "educação cívica" que era ministrada por um agente da Polícia. Por isso aquilo que nós fazemos de forma quase aleatória, ao longo do ano, em que hoje vai o agente x falar sobre VD, amanhã vai outro falar de ciber*bullying*, depois outro sobre consumo de drogas, no caso da Polícia Holandesa, havia essa disciplina onde o polícia dava todos estes temas. Isto acaba por ser muito positivo para a imagem da Polícia, para a relação Polícia e jovens e depois concentramos num horário, não há necessidade de andarmos constantemente a criar constrangimentos nos horários das escolas. Existe a dificuldade em arranjar horários, porque é a questão do tempo da ação, o número de jovens, a faixa etária, para cumprir os objetivos da Direção Nacional. E assim não, está resolvido. Os jovens têm no horário semanal e sabe-se que aquela turma tem aulas com um polícia, onde vão ser falados vários assuntos, com avaliação, e um deles há-de ser os crimes no ciberespaço, a criação de perfis, a idade com que podem criar uma conta no *facebook*, etc., no entanto, *n* têm contas no *facebook*, com idade inferior, e não há controlo algum, basta aceitarem amizades, começar a conversar, criar laços com alguém e começam a acreditar, no seu racional, que é alguém das suas idades, por causa da fotografia. Então ao nível

dos jogos também acontece, crianças que jogam com pessoas que não conhecem de lado nenhum, comunicam com elas, adquirem um vocabulário menos apropriado. Se um pai pudesse ver quem está do outro lado, provavelmente ficaria chocado. Mas como é normal, todos fazem isso, não se tem uma noção exata dos perigos, nem as crianças, nem pelos vistos os próprios pais, porque não proíbem. Podíamos eventualmente pensar nesta hipótese, de haver no horário semanal da criança um espaço dedicado a isto, em que o interlocutor podia ser um agente da PSP, onde tudo isto era lecionado, ganhávamos várias frentes: trabalhar a imagem da Polícia, a relação com os jovens, desconstruir a imagem da Polícia, sobretudo junto dos jovens que têm uma imagem mais negativa. A verdade é que através deste trabalho dos MIPP, consegue-se depois criar laços, se bem que depois estas crianças começam a olhar para estes polícias não como os polícias, mas como polícias diferentes, que não são bem polícias, como se houvesse os polícias bons e os maus. Há os "polícias polícias" e depois há estes que são da Escola Segura, que são diferentes, isso também não queremos. Eles são polícias, se sinalizarem alguma situação menos correta também têm de atuar. Mas às vezes, a ideia é que "ah mas se eu vou atuar…tenho de fechar os olhos de vez em quando, senão depois perco os laços e a confiança".

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: É um lugar-comum que onde se deve começar é pelos mais novos, mas ainda se pode fazer algum trabalho juntos dos pais e aí, normalmente a Polícia não aposta. Apostamos muito nos jovens, as EPES apostam imenso nestes, através das ações de sensibilização, mas é muito raro por exemplo a Polícia aparecer em reuniões de pais, é muito raro. Quando é uma altura em que vai haver uma reunião de pais, "olhe já agora reserve-me os últimos minutos da reunião para falarmos um pouco" ou então a Polícia é convidada para as reuniões de pais ou para reuniões de professores, não quer dizer que tenha de estar presente em toda a reunião, mas haver uns minutos iniciais ou no fim onde a Polícia também devia ter acento. E quem diz pais diz os mais velhos, os mais idosos. Onde se tem de investir? Eu não vou dizer os jovens, porque já se investe muito neles, claro que devemos continuar a investir, mas onde não se investe e devia-se investir mais é nas camadas mais idosas, que são tanto ou mais vulneráveis que os mais jovens, mas normalmente a Polícia não trabalha esta franja da população. Desde logo, porque estamos a falar de adultos e muitos deles podem levar a mal que a Polícia se esteja a meter na sua vida, ou até se faz sentido um filho controlar onde é que um pai anda a navegar. A Polícia normalmente trabalha com idosos- "idosos em segurança"-, lembro-me que na altura, acompanhávamos os idosos no levantamento da reforma quando iam aos CTT, ou então aqueles que vivem sozinhos, a Polícia de vez em quando aparecia para ver se estavam bem, mas não nesta perspetiva do ciberespaço "o senhor tem *internet*?" "por onde anda a navegar?", "mostre-me lá", isto não fazemos. "Olhe tenha atenção, não meta conversa com senhoras muito mais novas que prometem muito", que por detrás está um esquema de burla: querem é que ele transfira dinheiro, que adquira bens e lhe ofereça coisas, muitas vezes do outro lado nem está uma mulher, está um homem. Estas ciberburlas românticas têm vindo a crescer e nós somos uma população envelhecida e por isso é que eu costumo dizer que o nosso "cliente"/produto de segurança do futuro é o idoso. Sabemos isso, temos também de adaptar o nosso foco, aquilo que é forma como oferecemos o nosso produto e direcioná-lo para esta franja, que ao nível do ciberespaço, ainda não é feito. E no entanto, temos cada vez mais idosos no ciberespaço. Temos de investir mais nesta franja, não sei como, porque numa escola é fácil chegar à escola e falar com centenas de alunos, como é que chegamos ao público-alvo dos idosos? Só se for aos lares, aos centros sociais, aos centros de dia. Se não for nestes espaços, como chegamos aos idosos? É mais difícil, muitos deles vivem sozinhos…imagine que quer fazer uma ação de sensibilização, como o faz?

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: Os riscos que correm ao navegar na *internet* são os mesmos que correm no mundo real também, com uma *nuance*: no mundo real conseguem perceber ou sinalizar mais rapidamente a ameaça, desde logo, quando numa escola por exemplo, há um rapaz que o insulta, sabe quem é o rapaz, no ciberespaço pode acontecer também, por isso se diz que no âmbito do ciber*bullying* há uma transposição daquilo que acontece no mundo real para o ciberespaço, a criança nunca se liberta desses muros. No meu tempo, uma criança podia ser vítima de *bullying*, ser perseguido e humilhado por outra, mas isso morria quando saíamos da escola, hoje em dia não, a criança é vítima de *bullying* no espaço físico, chega a casa e continua a ser vítima no ciberespaço. Mas quer num caso, quer noutro conseguem identificar o agressor, não se diferenciando a ameaça em ambos os casos. Se tivéssemos de distinguir perigos que ocorrem no ciberespaço do mundo físico, faz sentido falarmos na questão dos predadores. Numa escola, conseguimos ver a pessoa, identificá-la, associá-la, porque somos feitos de rótulos "olha esta tem umas características que geram desconfiança", "eu sei quem ele é, ele dá-se com aquele grupo", portanto logo à partida, leva-nos a ter uma determinada conduta de algum cuidado, um pé atrás. Quando estamos à mercê do contacto ou disponíveis para falar com qualquer pessoa sem a conhecer, no ciberespaço, a tendência é isso não acontecer. E é com jovens, mas também com adultos. O não ver as pessoas dá aso também a uma abertura e disponibilidade para falar, que no contexto físico isso dificilmente iria acontecer. Ora as crianças estão mais vulneráveis por esse motivo, porque também são mais inocentes que os

adultos, e mesmo assim temos tantos adultos que são enganados...imagine-se as crianças, que não têm defesas nenhumas à partida. Tirando as crianças que nascem em meios complicados, num contexto em que o perigo está sempre latente, ganha defesas que, por exemplo, uma criança que cresça em Beja não tem. A forma de ver o mundo é inocente e quando mergulha no ciberespaço também o é, e quando lhe aparece uma cara da mesma idade do outro lado, com conversas infantis, acredita que é um possível amigo. Os perigos que a criança tem acabam por ser os mesmos que encontra no mundo físico, mas potenciados pela inocência própria da idade e depois também pela falta de supervisão. Se não houver supervisão parental, tudo isto depois ganha uma dimensão muito mais grave e, infelizmente pelos vistos, quando olhamos para os números ficamos assustados, porque é sinal de que os pais não estão presentes ou também são muito inocentes e acreditam que não há grandes perigos. Dos diálogos que tenho com vários pais, dá-me a impressão de que não há controlo, tirando um ou outro casal que vai ao *youtube* e cria limitações de visualização, mas tenho dúvidas de que isso seja a regra. A imagem que eu tenho é que uma criança, hoje em dia, com 4 anos, pode aceder a *sites* pornográficos, ver tudo e mais alguma coisa e portanto a sua inocência desaparece muito cedo. Há coisas que se calhar só devia ter contacto muito mais tarde e não. E ainda a agravante de aquilo que ocorre no mundo físico muitas vezes depois é extrapolado para o mundo digital, há muitos relatos desses, de jovens que depois humilham e injuriam no ciberespaço. Acaba por ser uma dimensão muito mais perigosa.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: De uma conferência em que participei, na Assembleia da República em 2017 ou 2018, com o título "Resiliência digital", tomei nota das principais conclusões, por exemplo, aquela de que as futuras guerras mundiais vão começar por ciberguerras, o termo "*cyberarmagueden".* Não sei se podemos falar no futuro, porque já é muito presente, que é aquilo que vamos sentindo quando vemos, por exemplo, alguns incidentes, um deles até foi com o grupo Empresa, com a SIC, portanto há este lado negativo, que tem a ver com os ciberataques, ciberameaças, do anonimato. Provavelmente vamos ter que chegar a um ponto em que teremos de permitir que haja ciberpoliciamento. Acho difícil, mas é provável que lá cheguemos, ou seja, qualquer cidadão perceber que aquilo que está a visitar, ao fim ao cabo é o que acontece no *facebook,* porque não há dúvidas que a sede do *facebook*, se quiser saber por onde navega o Nuno, que fotos é que foi ver, que imagens é que enviou pelo *messenger*, consegue fazê-lo e nós sabemos que isso acontece. Na prática, por muito que nos choque o ciberpoliciamento, pensar que haja alguém que tenha noção por onde eu ando a navegar, na verdade isso já acontece, optamos é por não pensar nisso. Ou por exemplo, se dissessem assim "olhe que as pessoas têm noção de quem visita a sua página", se calhar eu retraía-me por saber que a pessoa ia saber. Quando me aparece publicidade é toda ela canalizada em função do meu perfil, é inteligência artificial, quer dizer que alguém controla isso. Na prática isso já acontece, não queremos é que seja alguém que diga que é polícia, ou seja que é o Estado que está a controlar os seus comportamentos.

O grande desafio vai ser de facto mitigar aquilo que são as ameaças, que não sei se algum dia vai ser possível, também é impossível dizer que conseguimos controlar todo o crime nas ruas, o mesmo acontece no ciberespaço. Agora, não tenho dúvidas que conseguimos mitigar os danos, se conseguirmos aumentar a resiliência digital, as pessoas saiam das escolas mais esclarecidas, os idosos sejam mais esclarecidos. Provavelmente se tivéssemos um ciberpoliciamento, à semelhança do que acontece nas ruas, essas ameaças também eram mais mitigadas, tenho é dúvidas que isso aconteça agora. Tal como aconteceu com a videovigilância, vão é ter de morrer mais pessoas, polícias, para chegarmos à conclusão de que há aqui um bem superior que é a segurança de todos. O desafio é tentar, de facto, com aquilo que já existe ao nível da prevenção, ao nível da sinalização de comportamos desviantes, nas esferas em que isso é possível fazer-se e analisar, mitigar as ameaças, que são crescentes.

Informador qualificado 5

Cargo: Intendente, Diretor do Departamento de Operações, Coordenador do Policiamento de Proximidade e Oficial de Direitos Humanos da PSP

Data: 10 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: A pergunta está bem formulada, existem de facto duas áreas em que nós, PSP, podemos atuar: a prevenção e o combate. O combate, neste momento, na PSP, está sediado num Núcleo, que pertence ao Departamento de Investigação Criminal e, em concreto não é a nossa área de especialidade. Sobre essa matéria não me vou alongar muito. Naquilo que diz respeito à prevenção parece-me que efetivamente temos aqui algum caminho a percorrer ainda. Aliás julgo que é um caminho que ainda é toda uma descoberta porque infelizmente como temos visto nos últimos tempos a dinâmica e a criatividade das pessoas que se dedicam ao cibercrime é muito grande. Debate-se hoje se efetivamente não existirão organizações muito complexas e inclusivamente alguns estados a financiar esse tipo de atividades. Debate-se também se não é um novo palco de conflito entre estados e entre multinacionais que se transfere do público para o privado e do privado para o público, esbatendo as fronteiras que existiam e de que alguma forma nos ajudavam a definir as competências de cada um. Nós, PSP, em concreto na área da prevenção, trabalhamos sempre junto do público mais jovem e começo logo pelo que podemos fazer para alertar para os procedimentos de autoproteção. Na área da prevenção escolar em concreto, a PSP começa a trabalhar esta temática logo no primeiro ciclo, com ações de sensibilização em que alertamos os mais jovens para a necessidade de terem cuidado com os videojogos que vão colocando sobretudo nos telemóveis e nos *tablets*, que são os instrumentos que mais utilizam. Algum cuidado também com as redes sociais, algumas pessoas já começam a integrar o mundo virtual, terem cuidado com os anúncios que aparecem, não fazerem amizades, a não ser com pessoas que conheçam, sempre que tiverem dúvidas procurarem a supervisão e o auxílio dos adultos, enfim, começar com estas temáticas muito orientados para os jogos e para os vídeos que eles visualizam. A partir do segundo e terceiro ciclos já reforçamos mais alguns conselhos nas redes sociais: a necessidade de ter palavras fortes de segurança, a necessidade de não partilhar imagens que identifiquem os locais e outras pessoas, sobretudo, muito importante sempre não partilhar imagens íntimas. Enfim e alguns conselhos depois nos próprios procedimentos para garantir a segurança dos dispositivos e do *software* que utilizam. Para os mais velhos, para o ciclo secundário, então aí já estamos a trabalhar em temáticas um bocadinho mais profundas e, para isso também é importante dizer, é fundamental a cooperação que temos tido, no âmbito do Projeto Comunicar em Segurança com a formação PT, agora formação Altice que é nosso parceiro principal nesta abordagem e produção de conteúdos. Para além disso, e porque está também identificado como um público particularmente vulnerável, estamos a trabalhar os idosos, alertando-os também para os cuidados que têm de ter no manuseamento dos dispositivos quando estão na *internet*, seja para não entrar em anúncios ou compras *online* que possam ser fictícias e portanto eles poderem vir a ser vítimas de burlas; mas os cuidados também quando rececionam os *e-mails* com links que se percebam que possam ser maliciosos, com conteúdos também adulterados e que podem levar à prática de crimes; desconfiar sempre das ofertas que são demasiado tentadoras; enfim os conselhos genéricos que tentamos sensibilizar este público-alvo.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: A parte da investigação criminal não é connosco, não lhe posso responder, não sei.

3. Como se adaptou/adapta o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: Nesta altura, dando continuidade aos princípios do Policiamento de Proximidade, no que toca à prevenção que é feita no âmbito do MIPP, o policiamento do ciberespaço assume os mesmos contornos o policiamento físico, ou seja, é baseado na relação de confiança que os agentes vão estabelecendo com os alunos, em que, pontualmente vão interagindo com eles no espaço virtual, quando existe essa relação de proximidade, sem evadir nunca a intimidade de cada um, ma utilizando-se da rede de contactos físicos que existem, entre os amigos, os colegas, todos conhecem o agente, essa rede é depois transposta para o espaço virtual e é, por aí que o agente acaba por tomar contacto com algumas fragilidades dos próprios alunos, que muitas vezes, passam de forma indetetável no espaço físico mas que depois no espaço virtual eles podem vir ao de cima. Também é verdade que, fruto de alguns crimes estarem exclusivamente a ser cometidos em espaço virtual permite que os alunos consigam e, estão também sensibilizados para isso, cada vez mais obter prova e partilhar essa prova com os nossos agentes e reforçar depois os processos, em fase de inquérito, que nós temos de conduzir para o Ministério Público.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R:É muito sapiente trabalhar o ciberespaço e, não sendo eu, longe disso um perito na matéria, se no espaço físico nós conseguimos definir de uma forma mais clara as fronteiras entre o que é a intimidade e o que não é a intimidade, portanto os espaços públicos ou semipúblicos que nós possamos ter e frequentar, no ciberespaço isso é mais difícil de definir, e, para nós, polícias é um desafio ainda maior, porque nem sempre é claro o momento em que o jovem ou a pessoa idosa está a partilhar determinado conteúdo que não quer que se transforme numa denúncia criminal e dificulta o balanço entre a relação de confiança que nós temos de ter com a pessoa e o nosso dever enquanto Órgão de Polícia Criminal em participar crimes.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: É o tal dilema que falámos há pouco: o equilíbrio entre a privacidade, a confiança e o dever enquanto OPC de denunciar os crimes. É muito debilitado e é algo que precisa ainda de ser refletido e depois amadurecido para podermos ter orientações. Julgo que vai demorar algum tempo até conseguirmos isso.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: Nesta altura, o MIPP está fortemente implementado com base nas EPES e nas EPAV e isso, quer se queira, quer não condiciona a perceção que nós temos. É fácil nós respondermos que as equipas, ou as áreas de atuação da PSP que mais se disponibilizam para a prevenção do cibercrime são junto dos jovens e eventualmente sobretudo os idosos. Mas essa pode ser uma perceção que esteja inquinada, porque ela resulta do que nós fazemos e não das necessidades que nós ainda tivemos oportunidade de estudar com profundidade. Se calhar um estudo mais abrangente e com contributo de outras entidades que não apenas as Polícias podemos identificar outros grupos vulneráveis, com outras características que não sejam as etárias, que possam ter outro tipo de indicadores que sejam relevantes para a segurança interna e, em função disso, nós poderemos ter de reajustar. Nesta altura, aqueles que efetivamente mais contribuem são as equipas do Programa Escola Segura na sensibilização dos jovens e, para isso a PSP tem, pelo menos uma operação que anualmente realiza de âmbito nacional que é o *Internet* Mais Segura que terminou ontem (9FEV2022) e que teve mais uma edição neste ano letivo 21/22 e que fazemos todos os anos, procurando precisamente alertar para todos os ciclos escolares dos cuidados que é preciso ter para essa segurança no espaço virtual. Esta é reforçada com as recomendações que nós fazemos à população idosa, vamos também periodicamente produzindo publicações nas nossas redes sociais também para alertar quando percebemos que exista um maior espaço de receção por parte dos órgãos mais mediáticos e que a própria população, às vezes por casos que acontecem e que são difundidos na imprensa, que possam assim estar mais recetivos a alguma orientação que nós possamos dar e aí também quer algum dinamismo da nossa parte, mas repito há ainda muito para fazer.

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: O público que é sempre o principal são os mais jovens, porque são esses que, fruto de alguma ingenuidade e da exposição contínua a esse tipo de propostas acabam por estar em maior risco e, por isso são esses que nós temos de começar a trabalhar, até porque se a criança for desde cedo orientada a assumir comportamentos de autoproteção, estaremos a contribuir para que na fase adulta já esteja preparada para se proteger contra esse tipo de crimes. Portanto esse é sempre o primeiro público. Depois existem outros, se nós conseguíssemos identificar por exemplo as pessoas que têm problemas de adição ao jogo, poderia ser um público que nós pudéssemos trabalhar; se tivéssemos pessoas que têm algum problema de impulsividade em compras *online*, ou enfim, em partilha de determinados conteúdos que possam ser prejudicais para si próprios, também podemos trabalhar esses grupos, mas na falta de outros indicadores, trabalhemos com o que temos.

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: As crianças, propriamente ditas, e vamos aqui, se nos quisermos focar nas crianças que estão no primeiro ciclo (dos 6 aos 10 anos), os principais problemas tem a ver com a grande falta de controlo que existe na disseminação de conteúdos que possam ser perniciosos e não é nada difícil uma criança começar a ver um vídeo na plataforma *youtube* de desenhos animados comuns e passado dois minutos estar a ver um vídeo na mesma plataforma mas em que os conteúdos são extraordinariamente agressivos e até podem ser em desenhos animados mas em que as cenas de enorme violência com mortes, com utilização de armas, com sangue, com

enorme carga de agressividade são vulgares e isso é de facto preocupante porque passa a ideia, a criança acaba por estar repetidamente exposta a este tipo de estímulos, a não ser que os pais proíbam determinantemente a utilização de um instrumento que quer se queira quer não, é um instrumento de interação social, como é hoje o telemóvel. Mas se proibir os videojogos e se proibir a visualização de vídeos, uma criança de 6 a 10 anos, pouco mais poderá utilizar o telemóvel portanto a opção que se coloca é, ou vamos inibir as nossas crianças de poderem utilizar este tipo de recursos que mais cedo ou mais tarde vão ter de trabalhar com eles porque hoje em dia ela é imprescindível, ou então de facto correm riscos. A regulação parental e os instrumentos para essa regulação parental existem e devem ser do conhecimento dos pais e acionados por eles mas isso não dispensa a vigilância que os pais devem prestar, fazer e acompanhar as crianças naquilo que estão a ver. Ou seja, de 10 em 10 minutos, de 15 em 15 minutos devem ir confirmar o que os filhos estão a ver e pedir, isto também é importante, pedir para que as crianças descrevam o que estão a ver porque quando as crianças entram neste processo descritivo nós conseguimos ter uma melhor noção do impacto daquilo que elas estão a ver, do impacto que está a ter na própria criança. E se percebermos que aquilo pode ser perturbador e se a isso associarmos também a observação que fazemos em relação a uma eventual alteração comportamental que as crianças possam ter, isso pode ser um fator que tem de levar os pais a restringir a utilização destes dispositivos, seja no tempo de utilização em cada dia, seja por exemplo, só ao fim de semana ou de dois em dois dias, isso já depende de cada um. Depois temos outro tipo de condicionantes, o que nós estamos aqui a falar não tem a ver com o cibercrime, que passa pela necessidade que as crianças naturalmente têm da interação social presencial, o relacionamento físico e que quando passam muito tempo neste tipo de instrumentos acabam por perder faculdades de inter-relacionamento que se desenvolviam apenas na relação física. E muitas vezes isto também pode levar a problemas de controlo comportamental das próprias crianças por passarem muito tempo paradas naqueles dispositivos, podem acumular um excesso de energia que depois tem de ser extravasado em alguma forma e isso pode trazer influência no ambiente da sala de aula, mas também nas próprias famílias, porque depois os pais estão cansados no final do dia, as crianças ficaram 2h no telemóvel e depois querem andar a correr e querem atenção e os pais depois nessa altura já podem não ter tanta paciência quanto isso. Enfim, são desafios interessantes.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: Isso eu não sei responder. Gostava. Julgo que nesta altura, os países têm mesmo de se organizar para refletir sobre isso e explorar os vários cenários. Cenários, não apenas da segurança externa, muito virada para a ameaça do Estado e para proteção do Património que o Estado possa ter e estamos a falar apenas do património físico, mas no próprio espaço virtual as organizações não-governamentais, os organismos particulares devem também ter essa preocupação, mas é fundamental, parece-me que de uma vez por todas se encare a ameaça da cibercriminalidade, não apenas na vertente da segurança externa mas sobretudo a segurança interna e por segurança interna entenda-se aquela que atinge o indivíduo e não apenas a organização que apoia os indivíduos. Portanto as Polícias devem de facto ser envolvidas nesse processo, deve haver uma reflexão que se preocupe com a pessoa e não com o grupo de pessoas porque senão nós corremos o risco de não estarmos a direcionar para as fragilidades que as pessoas possam ter, direcionar as prioridades de prevenção que possam ser necessárias definir.

Informador qualificado 6

Cargo: Superintendente, Oficial de Ligação na Europol, antigo Coordenador do Policiamento de Proximidade da PSP

Data: 1 fevereiro 2022

1. No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?

R: O papel da PSP é importante, sobretudo ao nível da prevenção. Podemos desenvolver um papel bastante relevante na identificação de situações que configurem crimes ou outro tipo de atividades que, de certa forma, possam parecer atos preparatórios da prática de crimes. Também na sensibilização de determinados públicos-alvo, numa perspetiva mais ligada ao policiamento comunitário, quer seja na perspetiva das crianças

e dos jovens, dos adolescentes, quer dos idosos; portanto, um direcionamento para determinados tipos de público e determinado tipo de *modus operandi*.

Na perspetiva da investigação criminal, podemos igualmente desempenhar uma missão importante, designadamente na vertente das burlas consumadas com recurso a meios informáticos e, nessa perspetiva, para já e de acordo com a LOIC, esse é um dos principais campos de atuação, assim como a violência doméstica. Na violência doméstica, hoje em dia, um dos *modus operandi* que podem ser utilizados pelos agressores são os meios informáticos, por exemplo através de mensagens nas redes sociais ou a utilização de imagens das vítimas para as expor publicamente ou através de ameaças, etc. Esse também será outro campo importante a desenvolver.

2. Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?

R: A PSP precisa de capacitar os seus recursos humanos em todas estas vertentes, quer enquanto analistas de conteúdos colocados na *internet* e nas redes sociais, em que precisamos de ter equipas de trabalho policiais que possam de alguma forma navegar na rede e poder identificar situações que configurem crimes, quer depois também, enquanto peritos forenses na área digital. A área forense digital está em grande evolução e nós também precisamos dessa vertente.

3. Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?

R: O policiamento tradicional, nomeadamente ao nível do policiamento de proximidade na PSP, tem-se conseguido adaptar muito bem, tendo em conta que têm sido desenvolvidos muitos conteúdos formativos e de sensibilização que são utilizados pelas equipas do Programa Escola Segura ou pelas Equipas de Proximidade e Apoio à Vítima na sensibilização de determinados públicos-alvo, alertando para os riscos de utilização da *internet*, para determinados tipos legais de crime e *modus operandi* de que as pessoas possam ser vítimas. Nesse campo temos desenvolvido um trabalho muito importante na área da prevenção e da sensibilização, com muitos conteúdos de qualidade, alguns desenvolvidos apenas e só pela PSP e outros desenvolvidos em parceria com diversas entidades externas.

No que respeita ao patrulhamento da *internet*/rede/digital, também temos desenvolvido, em áreas específicas, iniciativas muito relevantes, por exemplo no âmbito da prevenção da violência no desporto, em que se faz um trabalho de monitorização da rede para poder detetar situações de preparação de atos de violência ou de conteúdos que apelem à violência, ao racismo e à intolerância. Igualmente ao nível da investigação criminal se tem feito algum investimento nesta área, com a criação no Departamento de Investigação Criminal de um núcleo específico para a área do cibercrime, que tem vindo a desenvolver cada vez mais um trabalho de especialização, mas é preciso fazer mais. Nomeadamente, daquilo que tenho visto aqui na EUROPOL, há, hoje em dia, "autênticos exércitos" de polícias no *backoffice* a patrulhar a rede.

Praticamente todos os crimes, hoje em dia, têm uma dimensão digital, mesmo aqueles que são praticados prioritariamente no mundo físico, têm um *backoffice* digital, por exemplo ao nível do branqueamento de capitais, da difusão de conteúdos ilícitos, sejam eles no âmbito dos crimes sexuais, sejam eles ao nível do tráfico de droga, de armas, etc. Nós, PSP, temos também de trabalhar muito a este nível. Para além da capacitação dos polícias, eventualmente teremos de repensar as carreiras na própria PSP, no que respeita ao eventual recrutamento de peritos, especialistas que não sejam polícias, nos quadros da PSP. Aliás, é o que acontece na PJ, que tem uma carreira própria para peritos na área informática e talvez a PSP tenha que caminhar para isso.

4. Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?

R: Sim, existem particularidades. De facto é necessário ser criada *expertise* específica para navegar na *deep web*, na *dark net*, etc. Existem particularidades que só alguns peritos conseguem desenvolver e acabam por entrar em determinados fóruns ou *sites* na *dark web*. Mas, ao mesmo tempo, há uma ligação muito forte entre o mundo físico e a utilização da rede para a prática de crimes ou para a divulgação de conteúdos ou pagamentos, que é outra questão muito específica hoje. Por exemplo, o pagamento de algo que é adquirido no mundo físico, no mundo digital, com cripto moedas. Nesta perspetiva, é preciso ter conhecimentos muito particulares e é necessária formação. Neste contexto, uma Polícia como a nossa, para além do papel que já desempenha muito importante ao nível do policiamento de proximidade, da prevenção, é importante que formemos os nossos RH para podermos acompanhar a evolução exponencial que vai acontecendo no mundo digital, porque todos os dias surgem novos *softwares*, novas ferramentas informáticas, novos *modus operandi*, sendo fundamental conseguir acompanhar esta evolução avassaladora da realidade.

5. Quanto controlo *online* é necessário e quando é demasiado?

R: Os Estados de Direito Democrático para se protegerem têm de ter controlo *online* mas dentro das regras do Direito. Ou seja, não pode valer tudo, porque se valer tudo estaremos a violar princípios fundamentais consignados no nosso enquadramento jurídico. No entanto, o prato da balança não pode pender só para a salvaguarda dos direitos em prejuízo das ferramentas que os OPC e a justiça têm de ter para poder investigar a criminalidade. Este prato da balança, face ao desenvolvimento da tecnologia, hoje em dia, é muito complexo. Basta ver que, hoje, tecnicamente é possível sermos localizados através dos nossos telemóveis e isso de certa forma configura uma violação da nossa privacidade. Mas se não for dada a possibilidade, de acordo com as regras do direito, de os OPC poderem identificar um suspeito e o local onde ele está e a utilização que ele faz das redes sociais, etc., não conseguimos, em muitos casos levar estes arguidos à justiça, nomeadamente, em processos de investigação de criminalidade mais complexa. É um equilíbrio que tem de ser conseguido e constitui um dos grandes desafios das democracias dos nossos dias.

6. Em relação ao MIPP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?

R: As valências que melhor contribuem para a prevenção destes ilícitos são claramente todos os recursos que temos no quadro do MIPP, quer na vertente mais direcionada para as escolas, quer na vertente mais direcionada para outros públicos-alvo, como os idosos, as vítimas de violência doméstica, etc. São todos os RH que temos afetos a estas equipas, sendo eles considerados como generalistas. Na diretiva do MIPP está lá previsto que estes recursos têm de ser considerados como uma espécie de generalistas/especialistas, porque têm de cobrir um vasto espectro de temáticas, mas ao mesmo tempo, temos de lhes ministrar formação e ferramentas, para que consigam ter um conhecimento aprofundado sobre, por exemplo, os riscos de utilização sem regras da *internet* ou os cuidados que as pessoas têm de ter com a utilização do *mbway*. Temos que ter a capacidade, enquanto instituição, de dar formação a estes polícias que, sendo generalistas, têm de possuir um conhecimento mais aprofundado para poder fornecer com qualidade formação a estes públicos-alvo. No desenvolvimento dos conteúdos que fizermos para ministrar nas escolas, etc., podemos ter de recorrer a entidades externas para nos validarem os conteúdos formativos, isto é, para nos certificarem de certa forma esses conteúdos. Os conteúdos de formação não podem ser desenvolvidos por um Agente ou um Superintendente meramente com base na pesquisa que ele faz da bibliografia ou da *internet*. Alguns destes conteúdos são de tal maneira específicos que, para terem qualidade e serem transmitidos ao público externo, têm de ser certificados e desenvolvidos em parceria com entidades credenciadas.

7. Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.

R: Claramente as crianças e jovens e os idosos. As crianças e jovens porque são o futuro da nossa sociedade e são eles que serão os decisores daqui a uns anos e são os principais utilizadores das novas tecnologias em toda a sua amplitude. Hoje em dia, uma criança desde tenra idade, mesmo um bebé, está exposto à tecnologia e mais tarde, poderá vir a ser um perito. Essa exposição em demasia acaba também por poder possibilitar virem a ser potenciais vítimas. Por outro lado, tendo em conta o envelhecimento da nossa população e uma percentagem significativa de infoexcluídos em escalões etários mais elevados, é importante que também apostemos nos cidadãos idosos. Não só por questões de solidão, porque estão muitas vezes sozinhos em casa e não têm o apoio de familiares ou amigos, mas também por fatores psico-motores são potencialmente mais vítimas. São estes dois grandes escalões etários da nossa sociedade, em que a PSP deverá investir.

8. Quais os riscos que correm as crianças ao navegar na *internet*?

R: Os riscos são vários, desde a vertente mais direcionada para os crimes sexuais, às questões relacionadas com a própria privacidade. Por exemplo, ao exporem determinado tipo de informações na *internet* e ao revelarem dados importantes que tenham conhecimento por parte dos pais. Há uma imensidão de riscos a que as crianças podem estar expostas e o elencar destes principais perigos deverá ser uma missão da PSP para poder, desde logo, priorizar os conteúdos formativos que ministraremos no âmbito da Escola Segura.

9. Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

R: Os desafios são a velocidade da evolução das tecnologias e a complexidade. Esta velocidade é tremenda, hoje em dia, já se fala no *meta* universo e nos próximos anos vai aparecer uma nova realidade que poderá criar novos riscos, que é a dos universos paralelos/digitais, que podem ter um grande risco na alienação das pessoas. As pessoas podem preferir "viver" nesses universos paralelos, fictícios, do que no mundo real, podendo criar grandes problemas de dependência e de alheamento do mundo físico. Uma questão que deve ser muito

explorada nas nossas ações de formação são os riscos de dependência.
Outro fator relevante é a complexidade, uma vez que, cada vez mais, são necessários conhecimentos mais específicos para poder contrariar os *modus operandi* cada vez mais criativos por parte dos criminosos. Daí a necessidade de recrutamento de peritos externos, para além da necessidade que temos de formar os nossos recursos policiais internos.

Apêndice H- Questionário aplicado aos encarregados de educação de crianças a frequentar o 1º ciclo da Escola José Tagarro no Cartaxo e na Escola Manuel Coco em Odivelas

INQUÉRITO POR QUESTIONÁRIO

Este inquérito foi criado no âmbito de uma investigação que está a ser conduzida no Instituto Superior de Ciências Policiais e Segurança Interna.

Este estudo tem como objetivo perceber o grau de conhecimento dos pais/encarregados de educação de crianças que frequentam o 1º Ciclo em relação à exposição dos seus filhos/educandos à internet.

Os dados fornecidos são **confidenciais e anónimos**. A informação recolhida será exclusivamente utilizada para fins académicos. Alguma dúvida poderá ser colocada a Sara Pereira, endereço de *e-mail:* **saramtpereira4@gmail.com**

Instruções de preenchimento:

- Deve colocar uma cruz no quadrado que mais se adequa ao caso do seu educando;
- Após o preenchimento do questionário, entregar ao Professor de turma;
- Devolver no espaço máximo de **4 dias**;
- No caso de ter mais do que um educando nesta escola (6 aos 10 anos), preencher um questionário por cada criança.

Idade da criança (6 A 10 ANOS): _____

Sexo da criança: ☐ MASCULINO
☐ FEMININO

Ano de escolaridade da criança: ☐ 1ºano ☐ 2ºano ☐ 3ºano ☐ 4ºano

Habilitações literárias do/a encarregado/a de educação: ☐ Ensino Básico ☐ Ensino Secundário ☐ Licenciatura ☐ Mestrado ☐ Doutoramento

1. **Com que frequência a criança está *online* ou usa a internet nos seguintes dispositivos?**
(Por exemplo: enviar ou receber mensagens, navegar, conversar com amigos e familiares, carregar ou descarregar ficheiros, publicar fotos ou qualquer outra coisa que costuma fazer *online*.)
(ESCOLHA UMA RESPOSTA PARA CADA LINHA)

	Nunca	Raramente	Pelo menos uma vez por mês	Pelo menos uma vez por semana	Todos os dias ou quase	Várias vezes por dia	Não sei
Telemóvel / *Smartphone*							
Computador de mesa ou portátil							
Tablet							
Outro							

2. **Quanto tempo a criança costuma estar sozinha na *Internet*?**
(videojogos, redes sociais, *netflix*, *youtube*, etc.)

Num dia de semana:	**Num dia de fim-de-semana:**
☐ Pouco tempo ou nenhum	☐ Pouco tempo ou nenhum
☐ Cerca de meia hora	☐ Cerca de meia hora
☐ Cerca de 1 hora	☐ Cerca de 1 hora
☐ Cerca de 2 horas	☐ Cerca de 2 horas
☐ Cerca de 3 horas	☐ Cerca de 3 horas
☐ Cerca de 4 horas	☐ Cerca de 4 horas
☐ Cerca de 5 horas	☐ Cerca de 5 horas
☐ Cerca de 6 horas	☐ Cerca de 6 horas
☐ Cerca de 7 horas	☐ Cerca de 7 horas
☐ Cerca de 8 horas	☐ Cerca de 8 horas
☐ Não sei	☐ Não sei

3. **Que atividades o/a seu/sua educando/a mais pratica, usualmente, nos tempos livres?**

☐ Pratica desporto ou outras atividades físicas

☐ Joga videojogos

☐ Conversa e diverte-se com amigos *online*

☐ Faz atividades ao ar livre

☐ Conversa e diverte-se com amigos cara a cara

☐ Ajuda a família nas tarefas domésticas

☐ Faz os trabalhos de casa ou outras atividades escolares

4. **Após a exposição da criança às tecnologias de informação e comunicação, observa alguma destas alterações comportamentais?**

☐ A criança ficou sem dormir e sem comer por causa do tempo despendido.

☐ A criança fica aborrecida por não poder estar no telemóvel, *tablet* ou computador.

☐ A criança procura contornar o impedimento, indo em busca de outro aparelho eletrónico.

☐ A criança fica agressiva com a família.

☐ A criança ficou ansiosa e teve dificuldade em dormir devido ao tipo de conteúdo que visualizou.

5. Algumas destas situações aconteceram com a criança nos últimos doze meses?

	Não	Sim	Não sei
Recebeu mensagens (telemóvel, *tablet*, computador) desagradáveis ou que a magoaram			
Puseram a circular mensagens desagradáveis sobre ela, que ficaram à vista de todos			
Puseram-na de lado ou fora de um grupo na *internet*			
Recebeu ameaças na *internet*			
Teve de fazer coisas que não queria fazer			
Aconteceram-lhe outras coisas desagradáveis ou que a magoaram na *internet*			
Alguém usou as suas informações pessoais			
O dispositivo (telemóvel, *tablet*, computador) que a criança usa apanhou um vírus ou *spyware*			
Gastou demasiado dinheiro em jogos *online* ou em compras feitas numa aplicação			
Alguém criou uma página ou uma imagem sobre ela que era ofensiva			
Alguém descobriu onde a criança estava porque viu a sua localização no telemóvel			

6. Caso tenha respondido "sim" em alguma circunstância acima referida, o que fez em relação à situação ocorrida?

- ☐ Apresentou queixa nas autoridades (PSP, GNR, PJ, MP)
- ☐ Apresentou queixa ao professor de turma
- ☐ Falou diretamente com os envolvidos
- ☐ Não fez nada

7. No caso de ter apresentado queixa às autoridades, como classifica a resposta por parte destas autoridades policiais?

- ☐ Totalmente satisfatória
- ☐ Satisfatória
- ☐ Sem resposta
- ☐ Pouco satisfatória
- ☐ Nada satisfatória

8. Tem alguns cuidados no acesso da criança à *internet*?

- ☐ Instalei um *software* de registo do histórico da *internet*.
- ☐ Configurei um bloqueio das horas de acesso.
- ☐ Coloquei um filtro.
- ☐ Vigio, não a deixando sozinha.
- ☐ Apenas sensibilizo.

9. Quando a criança está a usar a *internet*, com que frequência faz o seguinte?

	Nunca	Quase nunca	Algumas vezes	Muitas vezes	Quase sempre
Encoraja-a a explorar e a aprender coisas na *internet*					
Sugere modos de usar a *internet* de forma segura					
Fala com a criança sobre o que ela faz *online*					
Ajuda quando alguma coisa a aborrece na *internet*					

10. Durante os últimos 12 meses aconteceu alguma destas situações?

- ☐ A escola onde tem o/a educando/a recebeu alguma visita da Escola Segura (Polícia de Segurança Pública) a sensibilizar sobre os riscos da *internet*.
- ☐ A criança tem aulas que ensinem a lidar com os riscos e benefícios da *internet*.
- ☐ A criança tem aulas onde sejam consolidadas as competências digitais.
- ☐ Procurou obter mais informação sobre como agir na *internet* para melhorar a cibereducação do seu educando/a.

11. No plano da prevenção da segurança *online*, na sua opinião, qual a principal ou principais medidas a serem concretizadas nesta escola?

☐ Mais investimento nas idas da Escola Segura à escola para falar de *cyberbullying*, violência *online*, entre outros riscos na *internet*.

☐ Maior proximidade da Polícia com os encarregados de educação (ações de sensibilização/formação).

☐ Maior proximidade da Polícia com os professores e restante comunidade escolar.

☐ Maior investimento na formação sobre a utilização da *internet* junto dos pais.

☐ Deixar ficar na sala de aula os computadores emprestados pelo Ministério.

☐ Outra.
Qual?_____

_____

_____

_____

Apêndice I- Grelhas de análise de conteúdo das entrevistas realizadas aos polícias da PSP

Nota prévia: Por motivo de sequência lógica na análise, os quadros 2 e 12 são repetidos aqui.

Quadro 1- Matriz cromática das unidades de contexto e de registo da questão n.º 1

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"A PSP tem um papel fundamental na prevenção do cibercrime."	1.1
	"A PSP tem tido um papel ativo nas redes sociais e meios de comunicação social alertando a população para os riscos existentes na utilização das novas tecnologias e da *internet*."	1.2
	"O combate é outra questão, julgo que a PSP tem outro papel; não quer dizer que no futuro não possa mudar, mas neste momento é mais na vertente preventiva."	1.3
2	"A PSP atua nos crimes ciber-instrumentais, ou seja nos crimes dito tradicionais, mas que contam com o auxílio de plataformas na *internet* ou às redes sociais ou a mensagens de correio eletrónico para serem cometidos."	1.4
	"No Núcleo de cibercriminalidade foram definidos os objetivos, ou seja dar apoio a toda a estrutura de IC no âmbito da prevenção, deteção e investigação deste tipo de crimes." " (…) formar o próprio efetivo do núcleo e começar a dar apoio à estrutura de IC; damos também apoio a entidades externas";	1.5
	" (…) a monitorização de fontes abertas e a realização de alertas operacionais para o público interno e externo"	1.6
	"Desde o início percebemos que a principal forma de se prevenir a cibercriminalidade e combatê-la é o esclarecimento e consciencialização da população para a utilização segura da *internet*, porque é muito difícil chegar aos autores dos crimes por constrangimentos diversos e legais.	1.2
3	"Na prevenção há sempre dois pilares importantes: as políticas de intervenção e a divulgação a nível do policiamento de primeira linha."	1.7
	"O que funciona melhor em termos de prevenção é o policiamento de proximidade, divulgar também nas redes sociais, que já tem sido feito, para as pessoas terem alguns cuidados."	1.2
	"Depois ainda na prevenção, é o ciberpatrulhamento a funcionar, que na PSP já começa a existir, ainda que de uma forma ainda rudimentar, para antever situações que possam vir a acontecer em termos criminais. Isto no domínio da prevenção, porque investigar também é prevenir."	1.6
	"No domínio do combate, é sinalizar as situações e investigá-las devidamente, com meios, com tecnologia, com recursos humanos, e isso é um caminho que ainda não está a ser feito."	1.8
4	"É justamente neste âmbito que a PSP se deve circunscrever mais, que é no campo da prevenção."	1.1

	"Aquilo que eu sei é que neste momento a PSP está, por exemplo no caso da VD, em que publicar fotos para atingir determinada pessoa, um ex-parceiro ou ex-parceira é enquadrável também no crime de VD, a desenvolver este tipo de inquéritos. E pelos vistos, neste momento também já vamos tendo alguma capacidade técnica, no Núcleo de Cibercriminalidade, que está a receber vários pedidos, quer nossos, quer do MP."	1.9
	"A minha convicção, justamente pela minha experiência profissional, foi de que nós PSP, não devíamos entrar por aquilo que é a investigação criminal nesta área, essa era a minha realidade, porque não tínhamos capacidade técnica nem legal para assumir esse tipo de processos-crime, salvo quando a tal exceção de o MP poder delegar noutros OPC crimes que são da competência de um determinado OPC, que é o caso da PJ. No entanto, a PSP neste momento, está a receber muitas solicitações nesse sentido".	1.3
5	"A pergunta está bem formulada, existem de facto duas áreas em que nós, PSP, podemos atuar: a prevenção e o combate."	1.10
	"Naquilo que diz respeito à prevenção parece-me que efetivamente temos aqui algum caminho a percorrer ainda."	1.11
	"Nós, PSP, em concreto na área da prevenção, trabalhamos sempre junto do público mais jovem (…) " "Na área da prevenção escolar em concreto, a PSP começa a trabalhar esta temática logo no primeiro ciclo, com ações de sensibilização (…) ". "Para além disso, e porque está também identificado como um público particularmente vulnerável, estamos a trabalhar os idosos, alertando-os também para os cuidados que têm de ter no manuseamento dos dispositivos quando estão na *internet* (…) "	1.2
	" (…) é fundamental a cooperação que temos tido, no âmbito do Projeto Comunicar em Segurança com a formação PT, agora formação Altice que é nosso parceiro principal nesta abordagem e produção de conteúdos."	1.12
	"O combate, neste momento, na PSP, está sediado num Núcleo, que pertence ao Departamento de Investigação Criminal e, em concreto não é a nossa área de especialidade."	1.9
6	"O papel da PSP é importante, sobretudo ao nível da prevenção."	1.1
	"Podemos desenvolver um papel bastante relevante na identificação de situações que configurem crimes ou outro tipo de atividades que, de certa forma, possam parecer atos preparatórios da prática de crimes."	1.8
	"Também na sensibilização de determinados públicos-alvo, numa perspetiva mais ligada ao policiamento comunitário, quer seja na perspetiva das crianças e dos jovens, dos adolescentes, quer dos idosos (…)."	1.2
	"Na perspetiva da investigação criminal, podemos igualmente desempenhar uma missão importante. " " (…) na vertente das burlas consumadas com recurso a meios informáticos e, nessa perspetiva, para já e de acordo com a LOIC, esse é um dos principais campos de atuação, assim como a violência doméstica."	1.13

Quadro 2- Categorização da questão n.º1: "No seu entender, qual é o papel da PSP (em que vertentes pode atuar) no combate e na prevenção do cibercrime?"

Categoria	Subcategorias	Unidades de Registo	Informadores Qualificados						Unidades de Enumeração	Resultados (%)
			1	2	3	4	5	6		
Papel da PSP na prevenção e no combate ao cibercrime	Prevenção	1.2. Papel fundamental	X			X		X	3	50%
		1.2. Esclarecimento e consciencialização das pessoas	X	X	X		X	X	5	83,3%
		1.7. Políticas de intervenção e divulgação a nível do policiamento de primeira linha			X				1	16,7%
		1.11. Caminho a percorrer ainda					X		1	16,7%
		1.12. Cooperação					X		1	16,7%
	Combate	1.3. Papel secundário	X			X			2	33,3%
		1.8. Sinalizar situações e investigá-las			X			X	2	33,3%
		1.9. Sediado no Núcleo de Cibercriminalidade				X	X		2	33,3%
		1.13. Missão importante						X	1	16,7%
	Ambos	1.4. Papel nos crimes ciber-instrumentais		X					1	16,7%
		1.5. Dar apoio à estrutura de IC no âmbito da prevenção, deteção e investigação deste tipo de crimes		X	X				2	33,3%
		1.6. Monitorização de fontes abertas e realização de alertas operacionais		X	X				2	33,3%
		1.10. Ação nas duas áreas, prevenção e combate						X	1	16,7%

Quadro 3- Matriz cromática das unidades de contexto e de registo da questão n.º 2

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"Através de uma cada vez melhor e maior formação e especialização dos polícias que trabalham nessa área."	2.1
	"Através de uma monitorização do ciberespaço, particularmente das redes sociais e de outro tipo de locais que são disponíveis na *internet* de acesso livre ao cidadão (…)."	2.2
	"Também temos de ter em atenção que tem de haver uma cooperação cada vez maior entre as entidades responsáveis pela investigação do cibercrime e as empresas responsáveis pelo armazenamento dos dados de tráfego."	2.3
	"Não nos podemos esquecer que o cidadão deve estar cada vez mais sensibilizado para a importância de denunciar os crimes e, por vezes o setor empresarial não faz tanto como devia fazer, não quer vincular uma imagem de vulnerabilidade e de não terem capacidade de as suas empresas assegurarem uma cibersegurança perante a opinião pública que devia ser o máximo dos máximos."	2.4
2	"Nós temos de ter ferramentas para trabalhar. Não basta só os conhecimentos teóricos, saber mexer em computadores, etc., é preciso ter algumas ferramentas de *hardware* e *software* que permitam auxiliar as pesquisas. Porque os criminosos também se socorrem dessas ferramentas e têm acesso a elas e utilizam algumas que não são lícitas."	2.5
	"Também é preciso um grande trabalho em rede, porque é preciso compreender que não basta só o trabalho da Polícia, é preciso também fazer parcerias com o setor privado, com o mundo académico e com o mundo científico, porque são eles que têm o *know-how*, são eles que têm os profissionais qualificados e também são eles que desenvolvem equipamentos e ferramentas (…)."	2.3
	"A PSP não tem capacidade para ter esses mesmos profissionais nem capacidade económica para adquirir ferramentas, nem para as desenvolver porque também não temos esse tipo de conhecimentos."	2.6
3	"Essa é uma responsabilidade que não é só da PSP, aliás a responsabilidade da PSP nesse domínio não é consensual, embora tenhamos alguns crimes praticados por ambiente digital em que a investigação recai sobre a PSP."	2.3
	"Como reforçar: é a sinalização (…) "	2.7
	" (…) recursos humanos devidamente formados que não há (…)."	2.1
	" (…) meios técnicos especiais de investigação criminal nestes casos que também não há (…) "	2.5
	"A PSP não está ainda preparada para esta realidade."	2.6
4	"Eu estou muito convicto que o nosso papel, quer da PSP, quer da GNR, porque acho que ainda estamos a percorrer um caminho que é muito embrionário em termos de investigação do ciberespaço, é a prevenção".	2.6
	"Reforçar as competências dos nossos homens que trabalham na estrutura da IC, ao nível da formação e em termos técnicos."	2.1
5	"A parte da investigação criminal não é connosco, não lhe posso responder, não sei."	2.8
6	"A PSP precisa de capacitar os seus recursos humanos em todas estas vertentes, quer enquanto analistas de conteúdos colocados na *internet* e nas redes sociais (…), quer depois também enquanto peritos forenses na área digital."	2.1

Quadro 4- Categorização da questão n.º2 “Como reforçar a capacidade de investigar os crimes cometidos em ambiente digital?”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Reforço da capacidade de investigação destes crimes	Principais fatores	2.1. Mais e melhor formação e especialização dos polícias	X		X	X		X	4	80%
		2.2. Monitorização do ciberespaço	X						1	20%
		2.3. Cooperação	X	X	X				3	60%
		2.4. Cultura de denúncia dos crimes	X						1	20%
		2.5. Necessidade de meios técnicos		X	X				2	40%
		2.6. PSP não tem capacidade		X	X	X			3	60%
		2.7. Sinalização			X				1	20%

Nota: O informador qualificado 5 não respondeu a esta questão: “A parte da investigação criminal não é connosco, não lhe posso responder, não sei.” (UR 2.8)

Quadro 5- Matriz cromática das unidades de contexto e de registo da questão n.º 3

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"É indiscutível que o ciberespaço deve ser alvo de uma monitorização recorrente, nas fontes mais disponíveis, abertas ao público; a monitorização das atividades, das redes sociais;"	3.1
	" (…) a possibilidade de capacidade técnica dos investigadores para descerem até à camada mais obscura da *internet*."	3.2
	"O policiamento é muito diferente daquilo que nós conhecemos nas cidades. No policiamento preventivo é mais difícil de atuar, tem de haver uma adaptação que sinceramente não conheço qual é o papel da PSP no gabinete mas deve passar por muito pela monitorização do ambiente digital, pela criação de mais informação (…)."	3.3
2	"O patrulhamento do ciberespaço, que nós chamamos de monitorização (…), vamos fazendo alguma no *nciber* (…). Quando existe um processo concreto ou um suspeito em concreto, faz-se a monitorização desse suspeito, noutros casos monitoriza-se um fenómeno, alguma situação que tenha interesse."	3.4
	"Não temos ainda a capacidade de outras Polícias, em que a monitorização das redes sociais é feita exclusivamente por equipas que só se dedicam a isso, porque isso exige um empenhamento constante. Nós ainda não temos essa capacidade em termos de RH para o fazer."	3.5
3	"Vamos necessitar de pessoas devidamente formadas e que a tempo inteiro naveguem na *dark web* ou na *internet* dita comum e sinalizem situações de potencial prática criminal. Um "patrulheiro" no ambiente digital, vai ter de criar uma história de cobertura, vai ter de criar ali um, que no momento chamam de avatar, vai ter de criar uma personagem e isso não se faz em dois dias, isso alimenta-se, às vezes durante meses ou anos. Tem de haver este conhecimento e essa predisposição (…)."	3.2
	"Agora eles sinalizam e eventualmente poderão ali fazer algumas diligências prévias de investigação, portanto tentar perceber ali um bocadinho mais, mas depois a competência deles cessa ali (…)."	3.4
	(…). É impraticável fazer patrulhamento com um computador todo ligado à rede comum porque qualquer indivíduo que anda na *dark net* tem conhecimentos mínimos de informática e vai detetar os IP´s, vai detetar a localização, isto não se faz assim. E a PSP, não está preparada em termos logísticos para este tipo de funções (…)."	3.6
4	"Eu não diria que neste momento nós fazemos um patrulhamento do ciberespaço, o que nós fazemos é trabalhar a fase pré-crime. Eventualmente existe ciberpoliciamento, mas direcionado para aquilo que é o trabalho das informações, e aí sim sabemos que há polícias que o seu dia-a-dia é navegar no ciberespaço para sinalizar ou projetar cenários. Podemos falar de ciberpoliciamento, na ótica de prever comportamentos e cenários."	3.7
	"Não propriamente com o efeito que nós falamos do policiamento tradicional, da visibilidade policial e em função da visibilidade policial haver aqui um efeito de retração das pessoas. Ou seja, haver alguém que está a pensar cometer um crime e sente a presença da PSP, isso não acontece no ciberespaço."	3.3
	"No futuro pode acontecer (…) quem acedesse a um determinado conteúdo que não devia, aparecia um alerta. Havia como que um polícia, um *big brother* sempre presente. Ou então como acontece, por exemplo com quem anda a visitar determinados sites que estão a ser monitorizados por parte da PJ, depois mais tarde vir a ser constituído arguido por sites de pornografia infantil ou outros. Mas aí já é na perspetiva de sinalizar quem comete crime e depois atuar junto dessa pessoa e não propriamente na ótica como olhamos o policiamento, da prevenção: visibilidade para prevenir."	3.8

5	"Dando continuidade aos princípios do Policiamento de Proximidade, no que toca à prevenção que é feita no âmbito do MIPP, o policiamento do ciberespaço assume os mesmos contornos do policiamento físico, ou seja, é baseado na relação de confiança que os agentes vão estabelecendo com os alunos, em que, pontualmente vão interagindo com eles no espaço virtual (…) e é, por aí que o agente acaba por tomar contacto com algumas fragilidades dos próprios alunos, que muitas vezes, passam de forma indetetável no espaço físico mas que depois no espaço virtual eles podem vir ao de cima."	3.9
	" (…) os alunos consigam e, estão também sensibilizados para isso, cada vez mais obter prova e partilhar essa prova com os nossos agentes e reforçar depois os processos, em fase de inquérito, que nós temos de conduzir para o Ministério Público."	3.10
6	"O policiamento tradicional, nomeadamente ao nível do policiamento de proximidade na PSP, tem-se conseguido adaptar muito bem, tendo em conta que têm sido desenvolvidos muitos conteúdos formativos e de sensibilização (…)."	3.11
	"No que respeita ao patrulhamento da *internet*/rede/digital, também temos desenvolvido, em áreas específicas, iniciativas muito relevantes, por exemplo no âmbito da prevenção da violência no desporto, em que se faz um trabalho de monitorização da rede para poder detetar situações de preparação de atos de violência ou de conteúdos que apelem à violência, ao racismo e à intolerância."	3.4
	"Igualmente ao nível da investigação criminal se tem feito algum investimento nesta área, com a criação no Departamento de Investigação Criminal de um núcleo específico para a área do cibercrime, que tem vindo a desenvolver cada vez mais um trabalho de especialização."	3.12
	"Mas é preciso fazer mais. Nomeadamente, daquilo que tenho visto aqui na EUROPOL, há, hoje em dia, "autênticos exércitos" de polícias no *backoffice* a patrulhar a rede. Para além da capacitação dos polícias, eventualmente teremos de repensar as carreiras na própria PSP, no que respeita ao eventual recrutamento de peritos, especialistas que não sejam polícias (…)."	3.5

Quadro 6- Categorização da questão n.º3 “Como se adaptou o policiamento tradicional a um espaço não físico e como se patrulha o ciberespaço?”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Monitorização do ciberespaço	Existência de “ciberpoliciamento”	3.4. Monitorização direcionada do ciberespaço		X	X			X	3	50%
		3.7. Direcionamento para o trabalho das informações				X			1	16,7%
	Importância	3.1. Monitorização recorrente do ciberespaço	X					X	2	33,3%
	Adaptação	3.2. Necessidade de capacidade técnica dos investigadores	X		X				2	33,3%
		3.8. Existência de alertas				X			1	16,7%
		3.9. Policiamentos com os mesmos contornos					X		1	16,7%
		3.10. Cultura de denúncia do crime e partilha de prova					X		1	16,7%
		3.11. Adaptação do policiamento tradicional ao ciberespaço						X	1	16,7%
		3.12. Trabalho de especialização						X	1	16,7%
	Dificuldades	3.3. Policiamento diferente do tradicional	X			X			2	33,3%
		3.5. Falta de capacidade da PSP em termos de RH		X				X	2	33,3%
		3.6. Falta de capacidade da PSP em termos logísticos			X				1	16,7%

Quadro 7- Matriz cromática das unidades de contexto e de registo da questão n.º 4

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"Não podemos patrulhar o ciberespaço da mesma forma como patrulhamos uma cidade."	4.1
	"O ciberespaço na sua definição prima é o espaço virtual, não tem fronteiras que permitam delimitar um espaço, que é virtual, portanto será difícil estabelecer uma consideração de uma jurisdição. Podemos falar apenas do ciberespaço de interesse nacional."	4.2
	"Está relacionado com a disponibilidade, a integridade e confidencialidade de toda uma estrutura interconectada e as infraestruturas vitais para a nossa nação. As particularidades são essas. Temos de ter em conta a particularidade do ambiente ciber."	4.3
2	"Sim, o ciberespaço é um espaço totalmente diferente dos espaços tradicionais de conflito (terra, mar e ar)."	4.4
	"Nós agora temos um espaço que não obedece a fronteiras, em que as pessoas têm a capacidade de se anonimizar ou mascarar a sua identidade, onde a informação circula rapidamente em grandes quantidades e é volátil."	4.5
	"As ferramentas que os cibercriminosos têm à disposição também são diferentes daquelas que um criminoso tradicional utiliza."	4.6
	"A forma de atuar no ciberespaço também não pode ser a mesma de atuar para os crimes tradicionais, se bem que também não nos podemos esquecer que todo o cibercriminoso tem uma identidade, é uma pessoa. E as pessoas, apesar de atuarem no ciberespaço, também cometem os seus erros depois no mundo terreno."	4.1
	"A investigação tradicional continua a ser importante, mas temos que adaptar as ferramentas e os métodos ao espaço que estamos a trabalhar, assim como o tipo de prova que é recolhida, neste caso prova digital."	4.7
3	"Há particularidades, claro que sim."	4.4
	"Quem quiser fazer patrulhamento e até investigação destes casos, tem de ter equipamentos, tem de ter uma estrutura criada, que ainda não existe."	4.7
	" (…) é completamente diferente de investigarmos outro tipo de criminalidade."	4.1
4	"Ao nível das informações, não se pode dizer que é propriamente um ciberpoliciamento, porque o que os nossos polícias das Informações fazem é justamente pesquisar, por exemplo, nas redes sociais, em fontes abertas (…). Não é o policiamento da forma como conhecemos, é um trabalho de análise. Por exemplo, vai haver uma manifestação de coletes amarelos, as informações recolhem tudo o que têm e não quer dizer que aquilo não vá ocorrer, não há aqui o trabalho que é desenvolvido no policiamento tradicional em que passa um carro patrulha ou um homem fardado e as pessoas deixam de cometer aquele comportamento. Não é isso que acontece. O que acontece é o trabalho de informações para colherem informações para fazer chegar ao decisor e apoiar a sua decisão."	4.1
5	"É muito sapiente trabalhar o ciberespaço (…)."	4.8
	" (…) se no espaço físico nós conseguimos definir de uma forma mais clara as fronteiras entre o que é a intimidade e o que não é a intimidade, portanto os espaços públicos ou semipúblicos que nós possamos ter e frequentar, no ciberespaço isso é mais difícil de definir"	4.1

	" (…) para nós polícias é um desafio ainda maior, porque nem sempre é claro o momento em que o jovem ou a pessoa idosa está a partilhar determinado conteúdo que não quer que se transforme numa denúncia criminal e dificulta o balanço entre a relação de confiança que nós temos de ter com a pessoa e o nosso dever enquanto Órgão de Polícia Criminal em participar crimes."	4.9
6	"Sim, existem particularidades."	4.4
	"É necessário ser criada *expertise* específica para navegar na *deep web*, na *dark net*, etc. Existem particularidades que só alguns peritos conseguem desenvolver e acabam por entrar em determinados fóruns ou *sites* na *dark web*."	4.7

Quadro 8- Categorização da questão n.º4 “Na sua perspetiva, existem particularidades a ter em conta no patrulhamento do ciberespaço ou deve ser considerado como apenas mais uma jurisdição ou contexto criminal?”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Especificidades a ter em conta na monitorização do ciberespaço	Especificidades de enquadramento de espaço	4.1. “Patrulhamento” do ciberespaço diferente do de um espaço físico	X	X	X	X	X		5	83,3%
		4.2. Espaço virtual, sem fronteiras	X						1	16,7%
		4.7. Criação de ferramentas e estrutura		X	X			X	3	50%
	Especificidades quanto à confidencialidade da informação e identidade	4.3. Disponibilidade, integridade e confidencialidade da informação	X						1	16,7%
		4.5. Capacidade de anonimizar e mascarar a identidade		X					1	16,7%
		4.6. Ferramentas dos cibercriminosos diferentes das de um criminoso tradicional		X					1	16,7%

Quadro 9- Matriz cromática das unidades de contexto e de registo da questão n.º 5

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"O controlo *online* é necessário, é inevitável. Para o bem da segurança e do funcionamento do nosso país, isso não há volta a dar."	5.1
	"Julgo que não é demasiado se não suspeitar contra as liberdades das pessoas (…) "	5.2
2	"Da parte das autoridades, não é um controlo propriamente dito, nós temos é que ter a possibilidade de conseguir chegar à identificação de quem comete crimes *online* (…). Não entendo que seja necessário andarmos a controlar o que as pessoas fazem na *internet*, o que eu defendo é que temos de ter a capacidade de conseguir identificar as pessoas que cometem crimes."	5.3
	"Tem de haver mecanismos legais que obriguem a que as operadoras, além de terem de verificar os dados de quem se regista, (…) deveria existir uma obrigatoriedade de, perante um crime, a operadora ser responsável e ter de fornecer os dados de quem tem registado e de quem está identificado com aquele IP."	5.4
	"Não é aconselhável que crianças tenham acesso livre à *internet* e os pais não saibam sequer com quem é que elas estão a falar ou tenham redes sociais e os pais não tenham conhecimento de quem é que são os seus amigos. Os pais têm de fazer esse controlo, têm de ter regras definidas."	5.5
3	"Essa é a grande questão que se coloca em tudo o que é IC: até onde é que está o limite entre aquilo que são os deveres da investigação e os Direitos Fundamentais das pessoas."	5.6
	"Vai sempre depender das repercussões que o crime tem e a Lei prevê isso, não há aqui nada para a qual a Lei não tenha previsão. Tem que haver proporcionalidade e adequação nos meios."	5.7
4	"O controlo só faz sentido nesta lógica, que é quando há condutas que estão sinalizadas como ilegais e que conseguimos circunscrevê-las quando fazemos essa análise."	5.8
	"O limite deve ser esse: havendo uma atuação policial, com respaldo desde logo legitimado pela AJ e circunscrita naquilo que são franjas do ciberespaço (…)."	5.6
5	"É um dos desafios que estava a falar, até que ponto é que nós nos precisamos de adaptar a transpor o policiamento que extravasa a mera prevenção criminal para o espaço virtual. É o tal dilema: o equilíbrio entre a privacidade, a confiança e o dever enquanto OPC de denunciar os crimes."	5.6
	"A PSP não tem uma estrutura consolidada para fazer este tipo de trabalho preventivo. Existe um trabalho que é feito no âmbito do DIC, mas na área da prevenção propriamente dita, são os agentes que, conforme se referiu, transpõem os princípios do policiamento físico para o espaço virtual, mas não existem, ao contrário do que acontece em outros países, equipas que apenas se dedicam a esse tipo de atividade. Aqui provavelmente é algo que nós precisamos de pensar e criar."	5.9
6	"Os Estados de Direito Democrático para se protegerem têm de ter controlo *online* mas dentro das regras do Direito."	5.1
	"O prato da balança não pode pender só para a salvaguarda dos direitos em prejuízo das ferramentas que os OPC e a justiça têm de ter para poder investigar a criminalidade. (…) se não for dada a possibilidade, de acordo com as regras do direito, de os OPC poderem identificar um suspeito e o local onde ele está e a utilização que ele faz das redes sociais, etc., não conseguimos, em muitos casos, levar estes arguidos à justiça, nomeadamente, em processos de investigação de criminalidade mais complexa."	5.3
	"É um equilíbrio que tem de ser conseguido e constitui um dos grandes desafios das democracias dos nossos dias."	5.6

Quadro 10- Categorização da questão n.º5 “Quanto controlo *online* é necessário e quando é demasiado?”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Controlo *online*	Necessidade	5.1. Existência de controlo *online*	X					X	2	33,3%
		5.3. Identificação de quem comete crimes *online*		X				X	2	33,3%
		5.4. Mecanismos legais de obrigatoriedade para as operadoras		X					1	16,7%
		5.5. Controlo parental		X					1	16,7%
		5.8. Apenas controlo seletivo				X			1	16,7%
		5.9. Equipas dedicadas a este controlo					X		1	16,7%
	Limites	5.2. Liberdades das pessoas	X						1	16,7%
		5.6. Equilíbrio entre os deveres da investigação e os Direitos Fundamentais das pessoas			X	X	X	X	4	66,7%
		5.7. Proporcionalidade e adequação dos meios			X				1	16,7%

Quadro 11- Matriz cromática das unidades de contexto e de registo da questão n.º 6

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"Na parte do MIPP, da Escola segura, que, para mim é a valência que mais tem contribuído para sensibilizar as camadas mais jovens."	6.1
	"Não tenho conhecimento se existem programas também a nível de *internet*, julgo que já vi alguma coisa em tempos também, para a sensibilização dos mais idosos."	6.2
	"Limitações, não vejo aqui, talvez não sejam feitas ações suficientes atualmente."	6.3
2	"As equipas de proximidade da PSP fazem um excelente trabalho."	6.4
	"Mas não basta trabalhar com as crianças, a vítima de cibercriminalidade pode ser qualquer pessoa, com qualquer idade. A atuação das equipas de proximidade nesta área tem de ser mais abrangente."	6.3
	"Também tem de existir uma sensibilização dos pais."	6.5
	"Tem de haver uma educação por parte dos professores também, para que consigam identificar sinais de alerta."	6.6
	"Consciencialização não só focada na vítima mas também na dissuasão dos potenciais criminosos."	6.7
3	"Eu não acredito que, no âmbito do MIPP se vá conseguir trabalhar este tipo de questões, a não ser eventualmente na difusão de comportamentos que sejam preventivos (…) "	6.8
	"Mas essa difusão tem de ser feita também de forma generalizada."	6.3
	" (…) mas o principal não é por aí, não vai ser por aí, o principal é nós termos uma estrutura de investigação criminal célere e eficaz. A estrutura deve estar na repressão."	6.9
4	"Temos o trabalho que é desenvolvido pelas EPES (…) ciber*bullying*, a ligação entre a violência no namoro e as redes sociais (…) "	6.1
	"Quando falamos na tal ausência de guardião, muito disto acontece justamente porque o guardião, neste caso, o pai ou a mãe, não exerce o seu poder de supervisão, de controlo parental."	6.5
	"Neste momento já temos, em quantidades industriais, ações de sensibilização que são feitas ao nível das várias escolas."	6.10
	"Podíamos eventualmente pensar nesta hipótese, de haver no horário semanal da criança um espaço dedicado a isto, em que o interlocutor podia ser um agente da PSP, onde tudo isto era lecionado, ganhávamos várias frentes: trabalhar a imagem da Polícia, a relação com os jovens, desconstruir a imagem da Polícia, sobretudo junto dos jovens que têm uma imagem mais negativa."	6.11
5	"Se calhar um estudo mais abrangente e com contributo de outras entidades que não apenas as Polícias podemos identificar outros grupos vulneráveis, com outras características que não sejam as etárias, que possam ter outro tipo de indicadores que sejam relevantes para a segurança interna e, em função disso, nós poderemos ter de reajustar."	6.3
	"Nesta altura, aqueles que efetivamente mais contribuem são as equipas do Programa Escola Segura na sensibilização dos jovens e, para isso a PSP tem, pelo menos uma operação que anualmente realiza de âmbito nacional que é o *Internet* Mais Segura.	6.1
	"Recomendações que nós fazemos à população idosa"	6.2
	"Vamos também periodicamente produzindo publicações nas nossas redes sociais."	6.12
6	"As valências que melhor contribuem para a prevenção destes ilícitos são	6.4

	claramente todos os recursos que temos no quadro do MIPP, quer na vertente mais direcionada para as escolas, quer na vertente mais direcionada para outros públicos-alvo, como os idosos, as vítimas de violência doméstica, etc.”	
	“Estes recursos têm de ser considerados como uma espécie de generalistas/especialistas, porque têm de cobrir um vasto espectro de temáticas, mas ao mesmo tempo, temos de lhes ministrar formação e ferramentas, para que consigam ter um conhecimento aprofundado (…). ”	6.13
	“No desenvolvimento dos conteúdos que fizermos para ministrar nas escolas, etc., podemos ter de recorrer a entidades externas para nos validarem os conteúdos formativos, isto é, para nos certificarem de certa forma esses conteúdos.”	6.14

Quadro 12- Categorização da questão n.º6 “Em relação ao MIIP, quais são as valências, limitações e obstáculos que contribuem melhor para a prevenção destes ilícitos?”

Categoria	Subcategorias	Unidades de Registo	Informadores Qualificados						Unidades de Enumeração	Resultados (%)
			1	2	3	4	5	6		
MIPP	Valências	6.1.Escola Segura	X			X	X		3	50%
		6.2. Sensibilização da população idosa	X				X		1	33,3%
		6.4. Todos os recursos no quadro do MIPP		X				X	2	33,3%
		6.5. Sensibilização dos pais		X		X			1	33,3%
		6.6. Educação dos professores		X					1	16,7%
		6.7. Dissuasão dos potenciais criminosos		X					1	16,7%
		6.10. Ações de sensibilização em grande número nas escolas				X			1	16,7%
		6.11. Aula lecionada por um polícia				X			1	16,7%
		6.12. Publicações nas redes sociais					X		1	16,7%
	Limitações e obstáculos	6.3. Ações insuficientes e pouco abrangentes	X	X	X		X		4	66,7%
		6.8. O trabalho do MIPP não é suficiente			X				1	16,7%
		6.9. A estrutura deve estar na repressão			X				1	16,7%
		6.13. RH devidamente formados						X	1	16,7%
		6.14. Necessidade de validação dos conteúdos formativos						X	1	16,7%

Quadro 13- Matriz cromática das unidades de contexto e de registo da questão n.º 7

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"Publico alvo: crianças, jovens e idosos."	7.1
	"As crianças têm de ser sensibilizadas para os perigos que existem na utilização da *internet*."	7.2
	"Os idosos também para serem informados e alertados para como devem proceder e se comportar na utilização desta fantástica ferramenta que veio alterar por completo a nossa sociedade."	7.3
2	"Sinceramente em todo o público-alvo. Qualquer pessoa, em qualquer faixa etária e de qualquer sexo, pode ser vítima de cibercrime."	7.4
	"Dependendo do tipo de crime que estejamos a falar, existe um público-alvo que prevalece. Em termos da dissuasão, aplica-se sobretudo aos mais novos. Depois a consciencialização para a utilização segura da *internet* e para os riscos que correm, tem de ser feita em várias idades (…)."	7.5
3	"O público-alvo deve começar nas crianças e jovens (…)."	7.6
	"Eu tenho filhos e percebo que há perigos e que eles não estão devidamente sensibilizados para algumas questões."	7.2
4	"É um lugar-comum que onde se deve começar é pelos mais novos (…)."	7.6
	"Mas ainda se pode fazer algum trabalho junto dos pais e aí, normalmente a Polícia não aposta."	7.7
	"Onde não se investe e devia-se investir mais é nas camadas mais idosas, que são tanto ou mais vulneráveis que os mais jovens, mas normalmente a Polícia não trabalha esta franja da população."	7.8
5	"O público que é sempre o principal são os mais jovens (…)."	7.6
	"Depois existem outros, se nós conseguíssemos identificar por exemplo as pessoas que têm problemas de adição ao jogo, poderia ser um público que nós pudéssemos trabalhar; se tivéssemos pessoas que têm algum problema de impulsividade em compras *online*, ou enfim, em partilha de determinados conteúdos que possam ser prejudicais para si próprios, também podemos trabalhar esses grupos, mas na falta de outros indicadores, trabalhemos com o que temos."	7.9
	" (…) são esses que, fruto de alguma ingenuidade e da exposição contínua a esse tipo de propostas acabam por estar em maior risco e, por isso são esses que nós temos de começar a trabalhar, até porque se a criança for desde cedo orientada a assumir comportamentos de autoproteção, estaremos a contribuir para que na fase adulta já esteja preparada para se proteger contra esse tipo de crimes."	7.2
6	"Claramente as crianças e jovens e os idosos."	7.1
	"As crianças e jovens porque são o futuro da nossa sociedade e são eles que serão os decisores daqui a uns anos e são os principais utilizadores das novas tecnologias (…). Essa exposição em demasia acaba também por poder possibilitar virem a ser potenciais vítimas."	7.2
	"Tendo em conta o envelhecimento da nossa população e uma percentagem significativa de infoexcluídos em escalões etários mais elevados, é importante que também apostemos nos cidadãos idosos. Não só por questões de solidão, (…),mas também por fatores psico-motores são potencialmente mais vítimas."	7.10

Quadro 14- Categorização da questão n.º7 “Na sua opinião, em que público-alvo se deve apostar para a sensibilização? Justifique.”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Público-alvo a apostar	Público-alvo	7.1. Crianças, jovens e idosos	X					X	2	33,3%
		7.6. Deve começar nas crianças e jovens			X	X	X		3	50%
		7.4. Em todo o público-alvo		X					1	16,7%
		7.7. Junto dos pais				X			1	16,7%
		7.9. Pessoas que têm problemas de adição ao jogo, problemas de impulsividade em compras *online* ou em partilha de conteúdos prejudiciais para si próprias					X		1	16,7%
	Justificação	7.2. Ingenuidade das crianças, exposição contínua e porque são o futuro	X		X		X	X	4	66,7%
		7.5. Depende do tipo de crime		X					1	16,7%
		7.8. Idosos são tanto ou mais vulneráveis que os mais jovens				X			1	16,7%
		7.10. Envelhecimento da população e uma percentagem de infoexcluídos						X	1	16,7%

Quadro 15- Matriz cromática das unidades de contexto e de registo da questão n.º 8

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"Estarem sujeitos a conteúdos inadequados para a idade, por exemplo, aos phishings, burlas, cyberbullying (…)."	8.1
	" (…) predadores sexuais."	8.2
	"Nomeadamente também fazerem *download* de programas que podem conter *malware* ou programas que estão sujeitos a direitos de autor (…)."	8.3
2	"Os riscos são muitos, principalmente a questão dos predadores *online* (…)."	8.2
	"As crianças não têm consciência dos riscos que correm, não estão alertadas para estas questões. Mesmo com os próprios pares, quando nós falamos, e acontece com a questão do ciber*bullying,* os jovens pensam que é só uma brincadeira, e não é, é um crime e tem consequências para o visado."	8.4
	"É esta consciencialização que é precisa, pelos pais e professores e que as equipas de proximidade também podem fazer. Tem de passar muito pela educação. Mesmo havendo um patrulhamento da Polícia na *internet* destinado a identificar predadores sexuais, é impossível prevenir se a própria pessoa se expuser aos riscos. Não há um polícia para cada criança, para cada utilizador da *internet*."	8.5
3	"Podem ser vítimas de crime de extorsão."	8.6
	"Navegam na *internet*, são inocentes, pensam que tudo o que publicarem só os amigos é que vão ver e que não há perigo nenhum. Eles não têm a medida do perigo (…)."	8.4
	"Mas também há o perigo físico dos crimes sexuais (…) mas não me parece que seja preocupante."	8.7
4	"Os riscos que correm ao navegar na *internet* são os mesmos que correm no mundo real também, com uma *nuance*: no mundo real conseguem perceber ou sinalizar mais rapidamente a ameaça (…)."	8.8
	"O não ver as pessoas dá aso também a uma abertura e disponibilidade para falar, que no contexto físico isso dificilmente iria acontecer. Ora as crianças estão mais vulneráveis por esse motivo, porque também são mais inocentes que os adultos, e mesmo assim temos tantos adultos que são enganados, imagine-se as crianças, que não têm defesas nenhumas à partida."	8.4
	"Se não houver supervisão parental, tudo isto depois ganha uma dimensão muito mais grave e, infelizmente pelos vistos, quando olhamos para os números ficamos assustados, porque é sinal de que os pais não estão presentes ou também são muito inocentes e acreditam que não há grandes perigos."	8.5
5	"Crianças que estão no primeiro ciclo (dos 6 aos 10 anos), os principais problemas tem a ver com a grande falta de controlo que existe na disseminação de conteúdos que possam ser perniciosos e não é nada difícil uma criança começar a ver um vídeo na plataforma *youtube* de desenhos animados comuns e passado dois minutos estar a ver um vídeo na mesma plataforma mas em que os conteúdos são extraordinariamente agressivos e até podem ser em desenhos animados mas em que as cenas de enorme violência com mortes, com utilização de armas, com sangue, com enorme carga de agressividade são vulgares e isso é de facto preocupante."	8.9
	"A regulação parental e os instrumentos para essa regulação parental existem e devem ser do conhecimento dos pais e acionados por eles mas isso não dispensa a vigilância que os pais devem prestar, fazer e acompanhar as crianças naquilo que estão a ver."	8.5

	"Depois temos outro tipo de condicionantes, o que nós estamos aqui a falar não tem a ver com o cibercrime, que passa pela necessidade que as crianças naturalmente têm da interação social presencial, o relacionamento físico e que quando passam muito tempo neste tipo de instrumentos acabam por perder faculdades de inter-relacionamento que se desenvolviam apenas na relação física. (…) também pode levar a problemas de controlo comportamental."	8.10
6	"Os riscos são vários, desde a vertente mais direcionada para os crimes sexuais (…)."	8.2
	" (…) às questões relacionadas com a própria privacidade."	8.11
	"O elencar destes principais perigos deverá ser uma missão da PSP para poder, desde logo, priorizar os conteúdos formativos que ministraremos no âmbito da Escola Segura."	8.12

Quadro 16- Categorização da questão n.º8 “Quais os riscos que correm as crianças ao navegar na *internet*?”

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Riscos que correm as crianças ao navegar na *internet*	De ordem psíquica	8.1. Sujeitos a conteúdos inadequados para a idade	X						1	16,7%
		8.10. Perda de faculdades de inter-relacionamento e problemas de controlo comportamental					X		1	16,7%
	De ordem criminal	8.2. Predadores sexuais	X	X				X	3	50%
		8.6. Podem ser vítimas de extorsão			X				1	16,7%
	De ordem tecnológica	8.3. *Download* de programas que podem conter *malware* ou sujeitos a direitos de autor	X						1	16,7%
		8.9. Falta de controlo existente na disseminação de conteúdos que possam ser perniciosos					X		1	16,7%
	De ordem material	8.4. Não consciência dos riscos que correm		X	X	X			3	50%
		8.11. Questões relacionadas com a própria privacidade						X	1	16,7%

Quadro 17- Matriz cromática das unidades de contexto e de registo da questão n.º 9

Informador Qualificado	Unidade de Contexto	Unidade de Registo
1	"No futuro que já está cá."	9.1
	"Com o 5G (…)."	9.2
	" (…) toda a interconectividade dos sistemas (…)."	9.3
	"Com as *fake news.*"	9.4
	"Os algoritmos (…)."	9.5
2	"Se a tecnologia evolui, os cibercriminosos também (…)."	9.6
	"Existem outros desafios que vão ser colocados, que têm a ver com a evolução da própria sociedade e com esta vivência e necessidade que temos de comunicar através das redes sociais e estar constantemente a viver a nossa vida *online*, porque queremos ter acesso a tudo no preciso instante em que precisamos das coisas. A *internet* das coisas (…). Quando falamos deste nível de conexão, não falamos só das nossas casas, mesmo a própria cidade, o mundo, está-se a organizar dessa forma."	9.3
	"Com a utilização do 5G pior ainda. Porque vem aumentar a velocidade da comunicação, vem permitir que a *internet* das coisas possibilite a conexão de muitos mais equipamentos em simultâneo e com as consequências que podem advir daí."	9.2
3	"No futuro não sei muito bem, sei que no presente nós já temos alguns problemas."	9.1
	" (…) não há em Portugal uma cultura de defesa a nível de cibercriminalidade. O choque tecnológico nunca se fez em Portugal e nas Polícias então é que não se fez mesmo."	9.7
	"Isto é um desafio, é preparar os recursos humanos para lidar com este tipo de situações. Arrisco-me a dizer que mais de metade do efetivo da Polícia é infoexcluído, sabe aceder a um computador claro que sim, mas perceber minimamente como as coisas funcionam, não percebe e eu acho que esse é o maior desafio."	9.8
	"O maior desafio, a nível da PSP, será (…) montar uma estrutura eficaz e isso vai ser muito difícil (…)."	9.9
4	"Não sei se podemos falar no futuro, porque já é muito presente."	9.1
	"Provavelmente vamos ter que chegar a um ponto em que teremos de permitir que haja ciberpoliciamento. Na prática isso já acontece, optamos é por não pensar nisso. Quando me aparece publicidade é toda ela canalizada em função do meu perfil, é inteligência artificial, quer dizer que alguém controla isso. Na prática isso já acontece, não queremos é que seja alguém que diga que é polícia, ou seja que é o Estado que está a controlar os seus comportamentos."	9.10
	"O grande desafio vai ser de facto mitigar aquilo que são as ameaças, que não sei se algum dia vai ser possível (…).	9.11
	"Agora, não tenho dúvidas que conseguimos mitigar os danos, se conseguirmos aumentar a resiliência digital (…)."	9.12
5	" (…) parece-me que de uma vez por todas se encare a ameaça da cibercriminalidade, não apenas na vertente da segurança externa mas sobretudo a segurança interna e por segurança interna entenda-se aquela que atinge o indivíduo e não apenas a organização que apoia os indivíduos."	9.11

	"As polícias devem de facto ser envolvidas nesse processo, deve haver uma reflexão que se preocupe com a pessoa e não com o grupo de pessoas porque senão nós corremos o risco de não estarmos a direcionar para as fragilidades que as pessoas possam ter, direcionar as prioridades de prevenção que possam ser necessárias definir."	9.13
6	"A velocidade da evolução das tecnologias. Esta velocidade é tremenda, hoje em dia já se fala no *meta* universo e nos próximos anos vai aparecer uma nova realidade que poderá criar novos riscos, que é a dos universos paralelos/digitais, que podem ter um grande risco na alienação das pessoas."	9.2
	"A complexidade, uma vez que, cada vez mais, são necessários conhecimentos mais específicos para poder contrariar os *modus operandi* cada vez mais criativos por parte dos criminosos."	9.6
	"Daí a necessidade de recrutamento de peritos externos (…) "	9.14
	" (…) necessidade que temos de formar os nossos recursos policiais internos."	9.8

Quadro 18- Categorização da questão n.º9 “Quais são os desafios que a cibercriminalidade colocará no futuro e como os ultrapassar?

Categoria	**Subcategorias**	**Unidades de Registo**	**Informadores Qualificados**						**Unidades de Enumeração**	**Resultados (%)**
			1	2	3	4	5	6		
Desafios da cibercriminalidade no futuro	Desafios	9.1. Num futuro que já é presente	X		X	X			3	50%
		9.2. Velocidade da informação	X	X				X	3	50%
		9.3. Interconectividade dos sistemas	X	X					2	33,3%
		9.4. *Fake news*	X						1	16,7%
		9.5. Algoritmos	X						1	16,7%
		9.6. Evolução do *modus operandi* dos cibercriminosos		X				X	2	33,3%
		9.7. Inexistência de uma cultura de defesa a nível da cibercriminalidade			X				1	16,7%
		9.11. Ameaças, principalmente na vertente da segurança interna				X	X		2	33,3%
	Como os ultrapassar	9.8. Formação dos nossos RH			X			X	2	33,3%
		9.9. Montar uma estrutura eficaz			X				1	16,7%
		9.10. Existência de ciberpoliciamento				X			1	16,7%
		9.12. Aumentar a resiliência digital				X			1	16,7%
		9.13. Reflexão que se preocupe com a Pessoa					X		1	16,7%
		9.14. Recrutamento de peritos externos						X	1	16,7%

Apêndice J- Análise estatística

Caracterização sociodemográfica das crianças e EE

Quadro 19- Idade da criança

Idade da criança					
		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	6	83	16,0	16,0	16,0
	7	157	30,2	30,2	46,2
	8	108	20,8	20,8	66,9
	9	117	22,5	22,5	89,4
	10	48	9,2	9,2	98,7
	11	5	1,0	1,0	99,6
	12	2	,4	,4	100,0
	Total	520	100,0	100,0	

Quadro 20- Sexo da criança

Sexo da criança				
		Frequência	Percentagem	Percentagem válida
	Masculino	258	49,6	49,6
	Feminino	262	50,4	50,4
	Total	520	100,0	100,0

Quadro 21- Ano de escolaridade da criança

Ano de escolaridade da criança					
		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	1ºano	118	22,7	22,7	22,7
	2ºano	170	32,7	32,7	55,4
	3ºano	94	18,1	18,1	73,5
	4ºano	138	26,5	26,5	100,0
	Total	520	100,0	100,0	

Quadro 22- Habilitações literárias dos EE

Habilitações literárias dos EE					
		Frequência	Percentagem	Percentagem válida	Percentagem acumulativa
Válido	Ensino Básico	81	15,6	15,6	15,6
	Ensino Secundário	252	48,5	48,5	64,0
	Licenciatura	152	29,2	29,2	93,3
	Mestrado	30	5,8	5,8	99,0
	Doutoramento	5	1,0	1,0	100,0
	Total	520	100,0	100,0	

Apuramentos simples das variáveis

Quadro 23- Apuramentos simples da variável "Frequência com que a criança está online no telemóvel, computador/portátil, *tablet* e consola"

		Telemóvel		**Computador**		***Tablet***		**Consola**	
		F	%	F	%	F	%	F	%
Válido	Nunca	112	21,5	182	35,0	224	43,1	97	18,7
	Raramente	88	16,9	118	22,7	84	16,2	8	1,5
	Pelo menos uma vez por mês	11	2,1	41	7,9	29	5,6	3	0,6
	Pelo menos uma vez por semana	121	23,3	109	21,0	79	15,2	7	1,3
	Todos os dias ou quase	166	31,9	62	11,9	92	17,7	15	2,9
	Várias vezes por dia	19	3,7	4	0,8	8	1,5	0	0
	Não sei	1	0,2	2	0,4	1	0,2	8	1,5
	Total	518	99,6	518	99,6	517	99,4	138	26,5
Omisso	Sistema	2	0,4	2	0,4	3	0,6	382	73,5
Total		520	100,0	520	100,0	520	100,0	520	100,0
		Moda: "todos os dias ou quase"		**Moda**: "nunca"		**Moda**: "nunca"		**Moda:** "nunca"	

Quadro 24- Apuramentos simples da variável " quanto tempo a criança costuma estar sozinha na *internet* num dia de semana"

Tempo que a criança fica sozinha na *internet* num dia de semana			
		F	%
Válido	Pouco tempo ou nenhum	220	42,3
	Cerca de meia hora	79	15,2
	Cerca de 1 hora	129	24,8
	Cerca de 2 horas	50	9,6
	Cerca de 3 horas	18	3,5
	Cerca de 4 horas	10	1,9
	Cerca de 5 horas	2	,4
	Cerca de 7 horas	1	,2
	Não sei	1	,2
	Total	510	98,1
Omisso	Sistema	10	1,9
Total		520	100,0

Quadro 25- Apuramentos simples da variável "Tempo que a criança passa sozinha na *internet* num dia de fim de semana"

Tempo que a criança fica sozinha na *internet* num dia de fim de semana			
		F	%
Válido	Pouco tempo ou nenhum	121	23,3
	Cerca de meia hora	37	7,1
	Cerca de 1 hora	98	18,8
	Cerca de 2 horas	112	21,5
	Cerca de 3 horas	67	12,9
	Cerca de 4 horas	30	5,8
	Cerca de 5 horas	22	4,2
	Cerca de 6 horas	9	1,7
	Cerca de 7 horas	3	,6
	Cerca de 8 horas	6	1,2
	Não sei	5	1,0
	Total	510	98,1
Omisso	Sistema	10	1,9
Total		520	100,0

Quadro 26- Apuramentos simples da variável "Atividades que a criança mais pratica nos tempos livres"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Atividades que a criança mais pratica nos tempos livres[a]	Pratica desporto ou outras atividades físicas	273	15,3%	52,8%
	Joga videojogos	198	11,1%	38,3%
	Conversa e diverte-se com amigos *online*	90	5,0%	17,4%
	Faz atividades ao ar livre	301	16,9%	58,2%
	Conversa e diverte-se com amigos cara a cara	204	11,4%	39,5%
	Ajuda a família nas tarefas domésticas	303	17,0%	58,6%
	Faz os trabalhos de casa ou outras atividades escolares	415	23,3%	80,3%
Total		1784	100,0%	345,1%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 27- Apuramentos simples da variável "Atividades que a criança mais pratica nos tempos livres"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Atividades que a criança mais pratica nos tempos livres[a]	Pratica desporto ou outras atividades físicas	247	13,3%	48,3%
	Joga videojogos	322	17,3%	63,0%
	Conversa e diverte-se com amigos *online*	430	23,2%	84,1%
	Faz atividades ao ar livre	219	11,8%	42,9%
	Conversa e diverte-se com amigos cara a cara	316	17,0%	61,8%
	Ajuda a família nas tarefas domésticas	217	11,7%	42,5%
	Faz os trabalhos de casa ou outras atividades escolares	105	5,7%	20,5%
Total		1856	100,0%	363,2%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 28- Apuramentos simples da variável "Alterações Comportamentais da criança após a exposição às TIC"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Alterações comportamentais[a]	A criança ficou sem dormir e sem comer por causa do tempo despendido	5	1,3%	1,7%
	A criança fica aborrecida por não poder estar no telemóvel, *tablet* ou computador	259	66,4%	85,5%
	A criança procura contornar o impedimento, indo em busca de outro aparelho eletrónico	76	19,5%	25,1%
	A criança fica agressiva com a família	31	7,9%	10,2%
	A criança ficou ansiosa e teve dificuldade em dormir devido ao tipo de conteúdo que visualizou	19	4,9%	6,3%
Total		390	100,0%	128,7%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 29- Apuramentos simples da variável "Alterações Comportamentais da criança após a exposição às TIC"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Alterações Comportamentais[a]	A criança ficou sem dormir e sem comer por causa do tempo despendido	515	23,3%	99,2%
	A criança fica aborrecida por não poder estar no telemóvel, *tablet* ou computador	261	11,8%	50,3%
	A criança procura contornar o impedimento, indo em busca de outro aparelho eletrónico	444	20,1%	85,5%
	A criança fica agressiva com a família	489	22,1%	94,2%
	A criança ficou ansiosa e teve dificuldade em dormir devido ao tipo de conteúdo que visualizou	501	22,7%	96,5%
Total		2210	100,0%	425,8%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 30- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Situações que aconteceram com a criança[a]	Recebeu mensagens (telemóvel, *tablet*, computador) desagradáveis ou que a magoaram	504	9,1%	98,2%
	Puseram a circular mensagens desagradáveis sobre ela, que ficaram à vista de todos	509	9,2%	99,2%
	Puseram-na de lado ou fora de um grupo na *internet*	496	8,9%	96,7%
	Recebeu ameaças na *internet*	504	9,1%	98,2%
	Teve de fazer coisas que não queria	502	9,1%	97,9%
	Aconteceram-lhe outras coisas desagradáveis ou que a magoaram na *internet*	509	9,2%	99,2%
	Alguém usou as suas informações pessoais	504	9,1%	98,2%
	O dispositivo (telemóvel, *tablet*, computador) que a criança usa apanhou um vírus ou *spyware*	492	8,9%	95,9%
	Gastou demasiado dinheiro em jogos *online* ou em compras feitas numa aplicação	506	9,1%	98,6%
	Alguém criou uma página ou uma imagem sobre ela que era ofensiva	512	9,2%	99,8%
	Alguém descobriu onde a criança estava porque viu a sua localização no telemóvel	508	9,2%	99,0%
Total		5546	100,0%	1081,1%

a. Grupo de dicotomia tabulado no valor 1.

Quadro 31- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Situações que aconteceram com a criança[a]	Recebeu mensagens (telemóvel, *tablet*, computador) desagradáveis ou que a magoaram	5	11,9%	16,7%
	Puseram-na de lado ou fora de um grupo na *internet*	8	19,0%	26,7%
	Recebeu ameaças na *internet*	3	7,1%	10,0%
	Teve de fazer coisas que não queria	5	11,9%	16,7%
	Aconteceram-lhe outras coisas desagradáveis ou que a magoaram na *internet*	2	4,8%	6,7%
	Alguém usou as suas informações pessoais	3	7,1%	10,0%
	O dispositivo (telemóvel, *tablet*, computador) que a criança usa apanhou um vírus ou *spyware*	11	26,2%	36,7%
	Gastou demasiado dinheiro em jogos *online* ou em compras feitas numa aplicação	4	9,5%	13,3%
	Alguém descobriu onde a criança estava porque viu a sua localização no telemóvel	1	2,4%	3,3%
Total		42	100,0%	140,0%

a. Grupo de dicotomia tabulado no valor 2.

Quadro 32- Apuramentos simples da variável "Situações que aconteceram com a criança nos últimos doze meses"

		Respostas		Percentagem de casos
		N (Não sei)	Percentagem	
Situações que aconteceram com a criança[a]	Recebeu mensagens (telemóvel, *tablet*, computador) desagradáveis ou que a magoaram	5	9,4%	14,3%
	Puseram a circular mensagens desagradáveis sobre ela, que ficaram à vista de todos	4	7,5%	11,4%
	Puseram-na de lado ou fora de um grupo na *internet*	9	17,0%	25,7%
	Recebeu ameaças na *internet*	5	9,4%	14,3%
	Teve de fazer coisas que não queria	6	11,3%	17,1%
	Aconteceram-lhe outras coisas desagradáveis ou que a magoaram na *internet*	2	3,8%	5,7%
	Alguém usou as suas informações pessoais	5	9,4%	14,3%
	O dispositivo (telemóvel, tablet, computador) que a criança usa apanhou um vírus ou spyware	10	18,9%	28,6%
	Gastou demasiado dinheiro em jogos *online* ou em compras feitas numa aplicação	3	5,7%	8,6%
	Alguém criou uma página ou uma imagem sobre ela que era ofensiva	1	1,9%	2,9%
	Alguém descobriu onde a criança estava porque viu a sua localização no telemóvel	3	5,7%	8,6%
Total		53	100,0%	151,4%

a. Grupo de dicotomia tabulado no valor 3.

Quadro 33- Apuramentos simples da variável "Ação tomada pelo EE relativamente à situação que aconteceu com a criança"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Ação tomada pelos EE[a]	Falou diretamente com os envolvidos	4	25,0%	25,0%
	Não fez nada	12	75,0%	75,0%
Total		16	100,0%	100,0%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 34- Apuramentos simples da variável "Ação tomada pelo EE relativamente à situação que aconteceu com a criança"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Ação tomada pelos EE[a]	Apresentou queixa nas autoridades (PSP, GNR, PJ, MP)	515	25,2%	100,0%
	Apresentou queixa ao professor de turma	515	25,2%	100,0%
	Falou diretamente com os envolvidos	511	25,0%	99,2%
	Não fez nada	503	24,6%	97,7%
Total		2044	100,0%	396,9%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 35- Apuramentos simples da variável "Cuidados do EE no acesso da criança à *internet*"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Cuidados dos EE[a]	Instalei um *software* de registo de histórico da *internet*	54	8,5%	11,3%
	Configurei um bloqueio das horas de acesso	88	13,8%	18,4%
	Coloquei um filtro *web*	90	14,2%	18,9%
	Vigio, não a deixando sozinha	329	51,7%	69,0%
	Apenas sensibilizo	75	11,8%	15,7%
Total		636	100,0%	133,3%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 36- Apuramentos simples da variável "Cuidados do EE no acesso da criança à *internet*"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Cuidados dos EE[a]	Instalei um *software* de registo de histórico da *internet*	465	23,7%	89,6%
	Configurei um bloqueio das horas de acesso	431	22,0%	83,0%
	Coloquei um filtro *web*	429	21,9%	82,7%
	Vigio, não a deixando sozinha	190	9,7%	36,6%
	Apenas sensibilizo	444	22,7%	85,5%
Total		1959	100,0%	377,5%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 37- Apuramentos simples da variável "Frequência com que o EE encoraja, sugere, fala e ajuda a criança quando esta está *online*"

		Encoraja-a a explorar e a aprender coisas na *internet*		**Sugere modos de usar a *internet* de forma segura**		**Fala com a criança sobre o que ela faz *online***		**Ajuda quando alguma coisa a aborrece na *internet***	
		F	%	F	%	F	%	F	%
Válido	Nunca	75	14,4	45	8,7	27	5,2	55	10,6
	Quase nunca	58	11,2	30	5,8	9	1,7	26	5,0
	Algumas vezes	192	36,9	118	22,7	87	16,7	90	17,3
	Muitas vezes	104	20,0	172	33,1	197	37,9	127	24,4
	Quase sempre	52	10,0	123	23,7	164	31,5	172	33,1
	Total	481	92,5	488	93,8	484	93,1	470	90,4
Omisso	Sistema	39	7,5	32	6,2	36	6,9	50	9,6
Total		520	100,0	520	100,0	520	100,0	520	100,0

Quadro 38- Apuramentos simples da variável "Situações que aconteceram com a criança e o EE nos últimos doze meses"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Situações que aconteram com a criança e o EE[a]	A escola recebeu alguma visita da Escola Segura (PSP) a sensibilizar sobre os riscos da *internet*	139	35,5%	51,3%
	A criança tem aulas que ensinem a lidar com os riscos e benefícios da *internet*	54	13,8%	19,9%
	A criança tem aulas onde sejam consolidadas as competências digitais	100	25,5%	36,9%
	Procurou obter mais informação sobre como agir na *internet* para melhorar a cibereducação do seu educando	99	25,3%	36,5%
Total		392	100,0%	144,6%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 39- Apuramentos simples da variável " Situações que aconteceram com a criança e o EE nos últimos doze meses"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Situações que aconteram com a criança e o EE[a]	A escola recebeu alguma visita da Escola Segura (PSP) a sensibilizar sobre os riscos da *internet*	381	22,6%	74,9%
	A criança tem aulas que ensinem a lidar com os riscos e benefícios da *internet*	466	27,6%	91,6%
	A criança tem aulas onde sejam consolidadas as competências digitais	420	24,9%	82,5%
	Procurou obter mais informação sobre como agir na *internet* para melhorar a cibereducação do seu educando	421	24,9%	82,7%
Total		1688	100,0%	331,6%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 40- Apuramentos simples da variável "Medidas a serem concretizadas na escola"

		Respostas		Percentagem de casos
		N (Sim)	Percentagem	
Medidas a serem concretizadas na escola[a]	Mais investimento nas idas da Escola Segura à escola para falar de *cyberbullying*, violência *online*, etc.	439	42,9%	90,3%
	Maior proximidade da Polícia com os EE (ações de sensibilização/formação)	174	17,0%	35,8%
	Maior proximidade da Polícia com os professores e restante comunidade escolar	182	17,8%	37,4%
	Maior investimento na formação sobre a utilização da *internet* junto dos pais	179	17,5%	36,8%
	Deixar ficar na sala de aula os computadores emprestados pelo Ministério	49	4,8%	10,1%
Total		1023	100,0%	210,5%
a. Grupo de dicotomia tabulado no valor 1.				

Quadro 41- Apuramentos simples da variável "Medidas a serem concretizadas na escola"

		Respostas		Percentagem de casos
		N (Não)	Percentagem	
Medidas a serem concretizadas na escola[a]	Mais investimento nas idas da Escola Segura à escola para falar de *cyberbullying*, violência *online*, etc.	81	5,1%	16,1%
	Maior proximidade da Polícia com os EE (ações de sensibilização/formação)	346	21,9%	68,7%
	Maior proximidade da Polícia com os professores e restante comunidade escolar	338	21,4%	67,1%
	Maior investimento na formação sobre a utilização da *internet* junto dos pais	341	21,6%	67,7%
	Deixar ficar na sala de aula os computadores emprestados pelo Ministério	471	29,9%	93,5%
Total		1577	100,0%	312,9%
a. Grupo de dicotomia tabulado no valor 2.				

Quadro 42- Apuramentos simples da variável “Medidas a serem concretizadas na escola”

Outras medidas			
		F	%
Válido	Criação de uma aplicação para as Escolas com conteúdos e entretenimento.	2	0,4
	Não permitir a entrada de telemóveis nas escolas do 1º e 2º ciclos.	1	0,2
	A escola deve bloquear todos os *sites* que não sejam para a formação do aluno a nível escolar.	2	0,4
	Criação de uma linha de apoio para dúvidas e alertas, acompanhamento e participar se houver abusos.	1	0,2
	Criação de uma disciplina no programa educativo acerca dos benefícios e dos riscos e perigos da *internet*.	13	2,5
	Deixar ficar o computador do Ministério na escola durante a semana e ir aos fins-de-semana para casa.	1	0,2
	Atividades conjuntas com a Polícia, pais e professores.	1	0,2
	Formação à equipa educativa.	1	0,2
	Total	22	4,2
Omisso	Sistema	498	95,8
Total		520	100,0

Quadro 43- Frequência em telemóvel, por idade da criança

			Idade por escalão		Total
			6-7	8-12	
Frequência em telemóvel	Nunca	Frequência	60	52	112
		% em Frequência em telemóvel	53,6%	46,4%	100,0%
		% em Idade_escalões	25,1%	18,6%	21,6%
	Raramente	Frequência	43	45	88
		% em Frequência em telemóvel	48,9%	51,1%	100,0%
		% em Idade_escalões	18,0%	16,1%	17,0%
	Pelo menos uma vez por mês	Frequência	6	5	11
		% em Frequência em telemóvel	54,5%	45,5%	100,0%
		% em Idade_escalões	2,5%	1,8%	2,1%
	Pelo menos uma vez por semana	Frequência	58	63	121
		% em Frequência em telemóvel	47,9%	52,1%	100,0%
		% em Idade_escalões	24,3%	22,6%	23,4%
	Todos os dias ou quase	Frequência	67	99	166
		% em Frequência em telemóvel	40,4%	59,6%	100,0%
		% em Idade_escalões	28,0%	35,5%	32,0%
	Várias vezes por dia	Frequência	5	14	19
		% em Frequência em telemóvel	26,3%	73,7%	100,0%
		% em Idade_escalões	2,1%	5,0%	3,7%
	Não sei	Frequência	0	1	1
		% em Frequência em telemóvel	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	0,4%	0,2%
Total		Frequência	239	279	518
		% em Frequência em telemóvel	46,1%	53,9%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 44- Teste qui-quadrado das variáveis frequência em telemóvel e idade

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	9,313[a]	6	,157
Razão de verossimilhança	9,856	6	,131
Associação Linear por Linear	6,802	1	,009
N de Casos Válidos	518		
a. 2 células (14,3%) esperavam uma Frequência menor que 5. A Frequência mínima esperada é ,46.			

Quadro 45- Frequência em computador, por idade da criança

			Idade por escalão		Total
			6-7	8-12	
Frequência em computador	Nunca	Frequência	105	77	182
		% em Frequência em computador	57,7%	42,3%	100,0%
		% em Idade_escalões	43,9%	27,6%	35,1%
	Raramente	Frequência	68	50	118
		% em Frequência em computador	57,6%	42,4%	100,0%
		% em Idade_escalões	28,5%	17,9%	22,8%
	Pelo menos uma vez por mês	Frequência	14	27	41
		% em Frequência em computador	34,1%	65,9%	100,0%
		% em Idade_escalões	5,9%	9,7%	7,9%
	Pelo menos uma vez por semana	Frequência	37	72	109
		% em Frequência em computador	33,9%	66,1%	100,0%
		% em Idade_escalões	15,5%	25,8%	21,0%
	Todos os dias ou quase	Frequência	14	48	62
		% em Frequência em computador	22,6%	77,4%	100,0%
		% em Idade_escalões	5,9%	17,2%	12,0%
	Várias vezes por dia	Frequência	0	4	4
		% em Frequência em computador	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	1,4%	0,8%
	Não sei	Frequência	1	1	2
		% em Frequência em computador	50,0%	50,0%	100,0%
		% em Idade_escalões	0,4%	0,4%	0,4%
Total		Frequência	239	279	518
		% em Frequência em computador	46,1%	53,9%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 46- Teste qui-quadrado das variáveis frequência em computador e idade

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	42,222[a]	6	,000
Razão de verossimilhança	44,883	6	,000
Associação Linear por Linear	36,667	1	,000
N de Casos Válidos	518		
a. 4 células (28,6%) esperavam uma Frequência menor que 5. A Frequência mínima esperada é ,92.			

Quadro 47- Frequência em *tablet*, por idade da criança

			Idade por escalão		Total
			6-7	8-12	
Frequência em Tablet	Nunca	Frequência	111	113	224
		% em Frequência em Tablet	49,6%	50,4%	100,0%
		% em Idade_escalões	46,4%	40,6%	43,3%
	Raramente	Frequência	45	39	84
		% em Frequência em Tablet	53,6%	46,4%	100,0%
		% em Idade_escalões	18,8%	14,0%	16,2%
	Pelo menos uma vez por mês	Frequência	12	17	29
		% em Frequência em Tablet	41,4%	58,6%	100,0%
		% em Idade_escalões	5,0%	6,1%	5,6%
	Pelo menos uma vez por semana	Frequência	33	46	79
		% em Frequência em Tablet	41,8%	58,2%	100,0%
		% em Idade_escalões	13,8%	16,5%	15,3%
	Todos os dias ou quase	Frequência	38	54	92
		% em Frequência em Tablet	41,3%	58,7%	100,0%
		% em Idade_escalões	15,9%	19,4%	17,8%
	Várias vezes por dia	Frequência	0	8	8
		% em Frequência em Tablet	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	2,9%	1,5%
	Não sei	Frequência	0	1	1
		% em Frequência em Tablet	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	0,4%	0,2%
Total		Frequência	239	278	517
		% em Frequência em Tablet	46,2%	53,8%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 48- Teste qui-quadrado das variáveis frequência em *tablet* e idade

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	12,359[a]	6	,054
Razão de verossimilhança	15,791	6	,015
Associação Linear por Linear	6,213	1	,013
N de Casos Válidos	517		
a. 4 células (28,6%) esperavam uma Frequência menor que 5. A Frequência mínima esperada é ,46.			

Quadro 49- Frequência em consola, por idade da criança

			Idade por escalão		Total
			6-7	8-12	
Frequência em Consola	Nunca	Frequência	45	52	97
		% em Frequência em Consola	46,4%	53,6%	100,0%
		% em Idade_escalões	75,0%	66,7%	70,3%
	Raramente	Frequência	5	3	8
		% em Frequência em Consola	62,5%	37,5%	100,0%
		% em Idade_escalões	8,3%	3,8%	5,8%
	Pelo menos uma vez por mês	Frequência	2	1	3
		% em Frequência em Consola	66,7%	33,3%	100,0%
		% em Idade_escalões	3,3%	1,3%	2,2%
	Pelo menos uma vez por semana	Frequência	2	5	7
		% em Frequência em Consola	28,6%	71,4%	100,0%
		% em Idade_escalões	3,3%	6,4%	5,1%
	Todos os dias ou quase	Frequência	5	10	15
		% em Frequência em Consola	33,3%	66,7%	100,0%
		% em Idade_escalões	8,3%	12,8%	10,9%
	Não sei	Frequência	1	7	8
		% em Frequência em Consola	12,5%	87,5%	100,0%
		% em Idade_escalões	1,7%	9,0%	5,8%
Total		Frequência	60	78	138
		% em Frequência em Consola	43,5%	56,5%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 50- Teste qui-quadrado das variáveis frequência em consola e idade

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	6,555[a]	5	,256
Razão de verossimilhança	7,086	5	,214
Associação Linear por Linear	3,913	1	,048
N de Casos Válidos	138		
a. 8 células (66,7%) esperavam uma Frequência menor que 5. A Frequência mínima esperada é 1,30.			

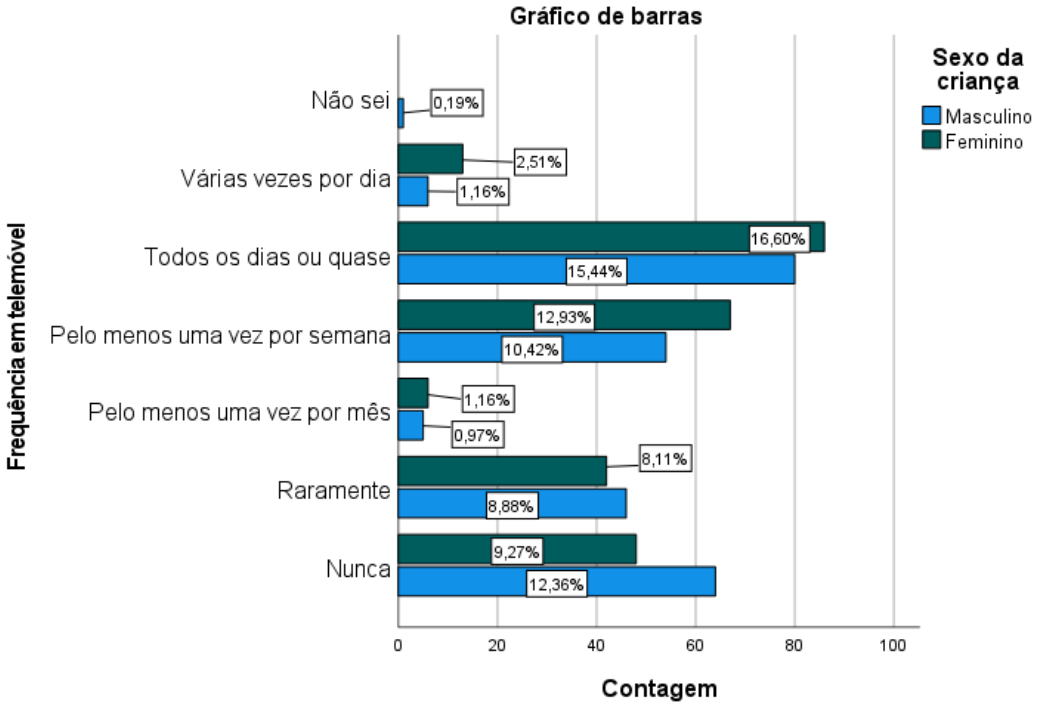


Gráfico 5- Frequência em telemóvel, por sexo da criança

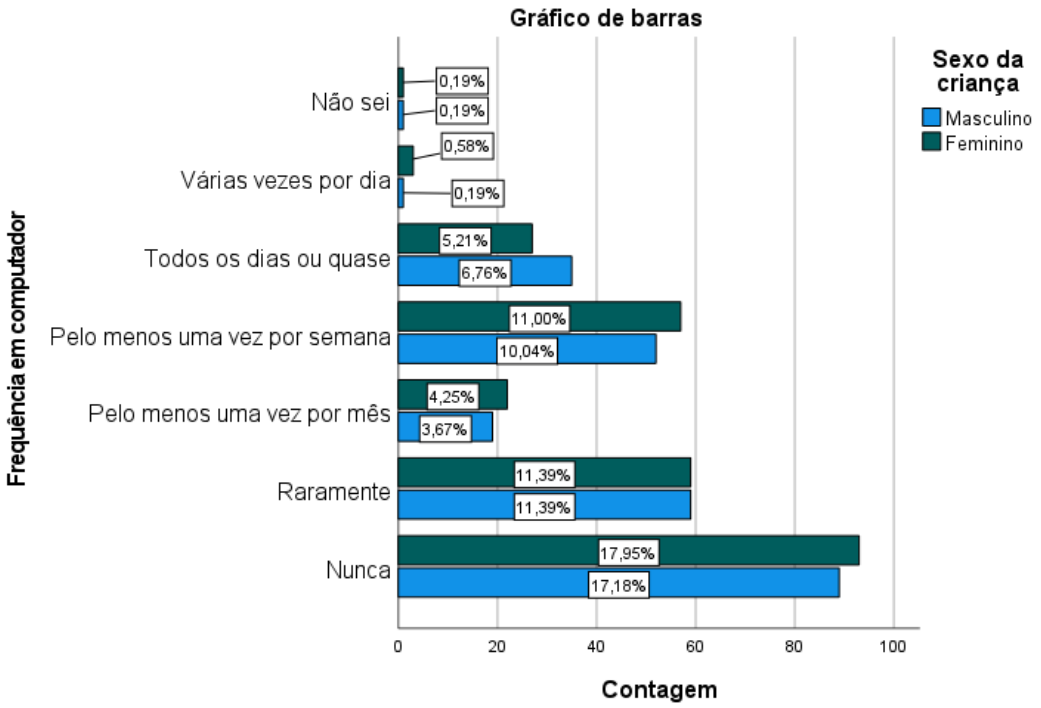


Gráfico 6- Frequência em computador, por sexo da criança

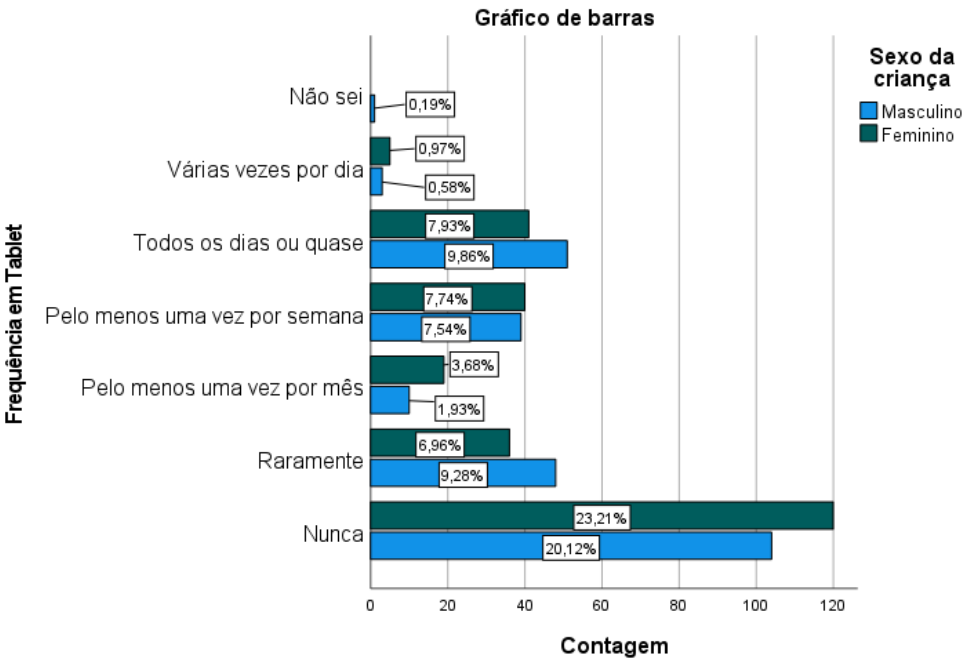


Gráfico 7- Frequência em tablet, por sexo da criança

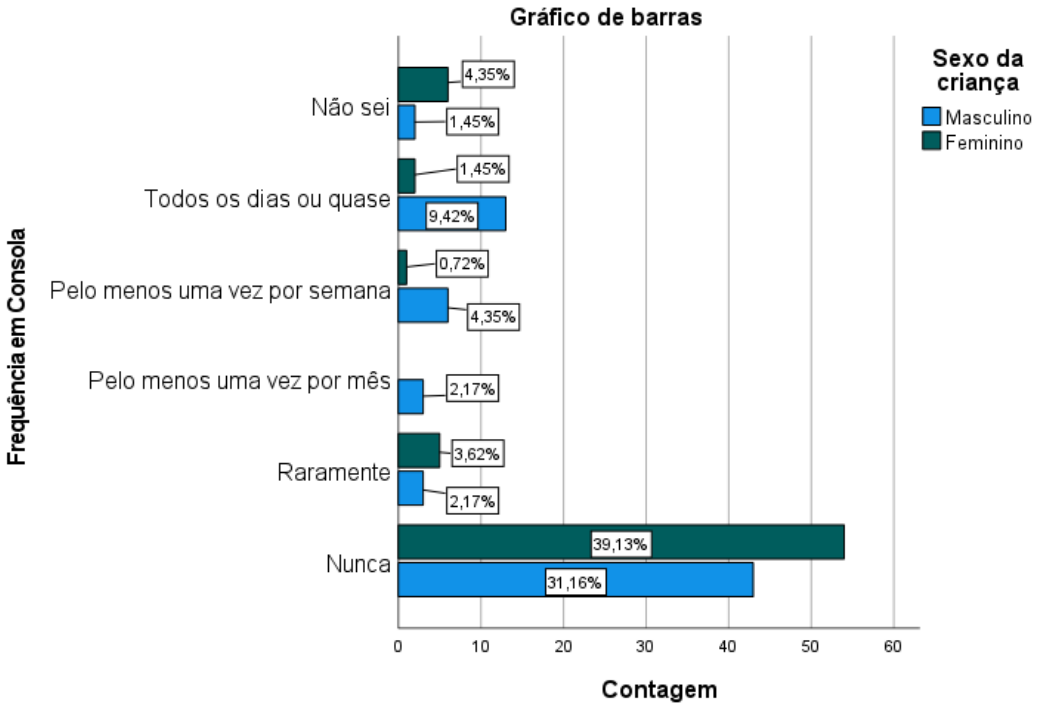


Gráfico 8- Frequência em consola, por sexo da criança

Quadro 51- Tempo que a criança fica sozinha na *internet* num dia de semana, por idade

			Idade por escalão		**Total**
			6-7	8-12	
Tempo que a criança fica sozinha na *internet* num dia de semana	Pouco tempo ou nenhum	Frequência	119	101	220
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	54,1%	45,9%	100,0%
		% em Idade_escalões	49,6%	37,4%	43,1%
	Cerca de meia hora	Frequência	39	40	79
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	49,4%	50,6%	100,0%
		% em Idade_escalões	16,3%	14,8%	15,5%
	Cerca de 1 hora	Frequência	57	72	129
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	44,2%	55,8%	100,0%
		% em Idade_escalões	23,8%	26,7%	25,3%
	Cerca de 2 horas	Frequência	17	33	50
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	34,0%	66,0%	100,0%
		% em Idade_escalões	7,1%	12,2%	9,8%
	Cerca de 3 horas	Frequência	2	16	18
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	11,1%	88,9%	100,0%
		% em Idade_escalões	0,8%	5,9%	3,5%
	Cerca de 4 horas	Frequência	4	6	10
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	40,0%	60,0%	100,0%
		% em Idade_escalões	1,7%	2,2%	2,0%
	Cerca de 5 horas	Frequência	1	1	2
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	50,0%	50,0%	100,0%
		% em Idade_escalões	0,4%	0,4%	0,4%
	Cerca de 7 horas	Frequência	1	0	1
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	100,0%	0,0%	100,0%
		% em Idade_escalões	0,4%	0,0%	0,2%
	Não sei	Frequência	0	1	1
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	0,4%	0,2%
Total		Frequência	240	270	510
		% em Tempo que a criança fica sozinha na *internet* num dia de semana	47,1%	52,9%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 52- Tempo que a criança fica sozinha na *internet* num dia de fim de semana, por idade

			Idade por escalão		Total
			6-7	8-12	
Tempo que a criança fica sozinha na *internet* num dia de fim de semana	Pouco tempo ou nenhum	Frequência	71	50	121
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	58,7%	41,3%	100,0%
		% em Idade_escalões	29,8%	18,4%	23,7%
	Cerca de meia hora	Frequência	20	17	37
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	54,1%	45,9%	100,0%
		% em Idade_escalões	8,4%	6,3%	7,3%
	Cerca de 1 hora	Frequência	50	48	98
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	51,0%	49,0%	100,0%
		% em Idade_escalões	21,0%	17,6%	19,2%
	Cerca de 2 horas	Frequência	45	67	112
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	40,2%	59,8%	100,0%
		% em Idade_escalões	18,9%	24,6%	22,0%
	Cerca de 3 horas	Frequência	31	36	67
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	46,3%	53,7%	100,0%
		% em Idade_escalões	13,0%	13,2%	13,1%
	Cerca de 4 horas	Frequência	9	21	30
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	30,0%	70,0%	100,0%
		% em Idade_escalões	3,8%	7,7%	5,9%
	Cerca de 5 horas	Frequência	5	17	22
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	22,7%	77,3%	100,0%
		% em Idade_escalões	2,1%	6,3%	4,3%
	Cerca de 6 horas	Frequência	4	5	9
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	44,4%	55,6%	100,0%
		% em Idade_escalões	1,7%	1,8%	1,8%
	Cerca de 7 horas	Frequência	1	2	3
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	33,3%	66,7%	100,0%
		% em Idade_escalões	0,4%	0,7%	0,6%
	Cerca de 8 horas	Frequência	2	4	6
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	33,3%	66,7%	100,0%

		% em Idade_escalões	0,8%	1,5%	1,2%
	Não sei	Frequência	0	5	5
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	0,0%	100,0%	100,0%
		% em Idade_escalões	0,0%	1,8%	1,0%
Total		Frequência	238	272	510
		% em Tempo que a criança fica sozinha na *internet* num dia de fim de semana	46,7%	53,3%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 53- Frequência com que a criança convive *online*, por idade

			Idade por escalão		**Total**
			6-7	8-12	
Conversa e diverte-se com amigos *online*	Sim	Frequência	9	81	90
		% em Conversa e diverte-se com amigos *online*	10,0%	90,0%	100,0%
		% em Idade_escalões	3,8%	28,9%	17,3%
	Não	Frequência	231	199	430
		% em Conversa e diverte-se com amigos *online*	53,7%	46,3%	100,0%
		% em Idade_escalões	96,3%	71,1%	82,7%
Total		Frequência	240	280	520
		% em Conversa e diverte-se com amigos *online*	46,2%	53,8%	100,0%
		% em Idade_escalões	100,0%	100,0%	100,0%

Quadro 54- Frequência com que a criança convive *online*, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Conversa e diverte-se com amigos *online*	Sim	% em Conversa e diverte-se com amigos online	50,0%	50,0%	100,0%
		% em Sexo da criança	17,4%	17,2%	17,3%
	Não	% em Conversa e diverte-se com amigos online	49,5%	50,5%	100,0%
		% em Sexo da criança	82,6%	82,8%	82,7%
Total		% em Conversa e diverte-se com amigos online	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 55- Frequência com que a criança convive cara a cara, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Conversa e diverte-se com amigos cara a cara	Sim	% em Conversa e diverte-se com amigos cara a cara	49,5%	50,5%	100,0%
		% em Sexo da criança	39,1%	39,3%	39,2%
	Não	% em Conversa e diverte-se com amigos cara a cara	49,7%	50,3%	100,0%
		% em Sexo da criança	60,9%	60,7%	60,8%
Total		% em Conversa e diverte-se com amigos cara a cara	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 56- Frequência com que a criança pratica desporto ou outras atividades físicas, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Pratica desporto ou outras atividades físicas	Sim	% em Pratica desporto ou outras atividades físicas	54,2%	45,8%	100,0%
		% em Sexo da criança	57,4%	47,7%	52,5%
	Não	% em Pratica desporto ou outras atividades físicas	44,5%	55,5%	100,0%
		% em Sexo da criança	42,6%	52,3%	47,5%
Total		% em Pratica desporto ou outras atividades físicas	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 57- Frequência com que a criança joga videojogos, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Joga videojogos	Sim	% em Joga videojogos	69,2%	30,8%	100,0%
		% em Sexo da criança	53,1%	23,3%	38,1%
	Não	% em Joga videojogos	37,6%	62,4%	100,0%
		% em Sexo da criança	46,9%	76,7%	61,9%
Total		% em Joga videojogos	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 58- Frequência com que a criança faz atividades ao ar livre, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Faz atividades ao ar livre	Sim	% em Faz atividades ao ar livre	51,2%	48,8%	100,0%
		% em Sexo da criança	59,7%	56,1%	57,9%
	Não	% em Faz atividades ao ar livre	47,5%	52,5%	100,0%
		% em Sexo da criança	40,3%	43,9%	42,1%
Total		% em Faz atividades ao ar livre	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 59- Frequência com que a criança ajuda a família, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Ajuda a família nas tarefas domésticas	Sim	% em Ajuda a família nas tarefas domésticas	47,9%	52,1%	100,0%
		% em Sexo da criança	56,2%	60,3%	58,3%
	Não	% em Ajuda a família nas tarefas domésticas	52,1%	47,9%	100,0%
		% em Sexo da criança	43,8%	39,7%	41,7%
Total		% em Ajuda a família nas tarefas domésticas	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%

Quadro 60- Frequência com que a criança faz os TPC ou outras atividades escolares, por sexo

			Sexo da criança		Total
			Masculino	Feminino	
Faz os trabalhos de casa ou outras atividades escolares	Sim	% em Faz os trabalhos de casa ou outras atividades escolares	48,4%	51,6%	100,0%
		% em Sexo da criança	77,9%	81,7%	79,8%
		% do Total	38,7%	41,2%	79,8%
	Não	% em Faz os trabalhos de casa ou outras atividades escolares	54,3%	45,7%	100,0%
		% em Sexo da criança	22,1%	18,3%	20,2%
		% do Total	11,0%	9,2%	20,2%
Total		% em Faz os trabalhos de casa ou outras atividades escolares	49,6%	50,4%	100,0%
		% em Sexo da criança	100,0%	100,0%	100,0%
		% do Total	49,6%	50,4%	100,0%

Quadro 61- Frequência com que a criança fica aborrecida por não estar nos dispositivos digitais, por idade

			Idade da criança							Total
			6	7	8	9	10	11	12	
A criança fica aborrecida por não poder estar no telemóvel, *tablet* ou computador	SIM	F	32	87	56	56	24	2	2	259
		% em A criança fica aborrecida	12,4%	33,6%	21,6%	21,6%	9,3%	0,8%	0,8%	100,0%
		% em Idade da criança	38,6%	55,4%	51,9%	47,9%	50,0%	40,0%	100,0%	49,8%
	NÃO	F	51	70	52	61	24	3	0	261
		% em A criança fica aborrecida	19,5%	26,8%	19,9%	23,4%	9,2%	1,1%	0,0%	100,0%
		% em Idade da criança	61,4%	44,6%	48,1%	52,1%	50,0%	60,0%	0,0%	50,2%
Total		F	83	157	108	117	48	5	2	520
		% em A criança fica aborrecida	16,0%	30,2%	20,8%	22,5%	9,2%	1,0%	0,4%	100,0%
		% em Idade da criança	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

Quadro 62- Cuidados do EE no acesso da criança à *internet*, por habilitações literárias

			Habilitações Literárias do EE			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Cuidados no acesso da criança à *internet*[a]	Instalei um *software* de registo de histórico da *internet*	F	4	25	25	54
		% em $Q8	7,4%	46,3%	46,3%	
		% em Hab_2	5,7%	10,9%	14,1%	
	Configurei um bloqueio das horas de acesso	F	8	39	41	88
		% em $Q8	9,1%	44,3%	46,6%	
		% em Hab_2	11,4%	17,0%	23,2%	
	Coloquei um filtro *web*	F	5	30	55	90
		% em $Q8	5,6%	33,3%	61,1%	
		% em Hab_2	7,1%	13,0%	31,1%	
	Vigio, não a deixando sozinha	F	50	165	114	329
		% em $Q8	15,2%	50,2%	34,7%	
		% em Hab_2	71,4%	71,7%	64,4%	
	Apenas sensibilizo	F	12	40	23	75
		% em $Q8	16,0%	53,3%	30,7%	
		% em Hab_2	17,1%	17,4%	13,0%	
Total		F	70	230	177	477

Percentagens e totais têm respondentes como base.

a. Grupo de dicotomia tabulado no valor 1.

Quadro 63- Cuidados do EE no acesso da criança à *internet*, por idade da criança

			Idade por escalão		Total
			6-7	8-12	
Cuidados no acesso da criança à *internet*[a]	Instalei um *software* de registo de histórico da *internet*	F	20	34	54
		% em $Q8	37,0%	63,0%	
		% em Idade_2	9,1%	13,2%	
	Configurei um bloqueio das horas de acesso	F	39	49	88
		% em $Q8	44,3%	55,7%	
		% em Idade_2	17,7%	19,1%	
	Coloquei um filtro *web*	F	41	49	90
		% em $Q8	45,6%	54,4%	
		% em Idade_2	18,6%	19,1%	
	Vigio, não a deixando sozinha	F	169	160	329
		% em $Q8	51,4%	48,6%	
		% em Idade_2	76,8%	62,3%	
	Apenas sensibilizo	F	20	55	75
		% em $Q8	26,7%	73,3%	
		% em Idade_2	9,1%	21,4%	
Total		F	220	257	477
Percentagens e totais têm respondentes como base.					
a. Grupo de dicotomia tabulado no valor 1.					

Quadro 64- Frequência com que o EE encoraja a criança a explorar na *internet*, por habilitação literária

			Habilitações Literárias do EE					Total
			Ensino Básico	Ensino Secundário	Licenciatura	Mestrado	Doutoramento	
Encoraja-a a explorar e a aprender coisas na *internet*	Nunca	F	17	38	16	2	2	75
		% em Encoraja-a	22,7%	50,7%	21,3%	2,7%	2,7%	100,0%
		% em HL do EE	22,1%	16,7%	11,3%	6,9%	40,0%	15,6%
	Quase nunca	F	5	30	18	4	1	58
		% em Encoraja-a	8,6%	51,7%	31,0%	6,9%	1,7%	100,0%
		% em HL do EE	6,5%	13,2%	12,7%	13,8%	20,0%	12,1%
	Algumas vezes	F	36	90	55	10	1	192
		% em Encoraja-a	18,8%	46,9%	28,6%	5,2%	0,5%	100,0%
		% em HL do EE	46,8%	39,5%	38,7%	34,5%	20,0%	39,9%
	Muitas vezes	F	12	50	30	11	1	104
		% em Encoraja-a	11,5%	48,1%	28,8%	10,6%	1,0%	100,0%
		% em HL do EE	15,6%	21,9%	21,1%	37,9%	20,0%	21,6%
	Quase sempre	F	7	20	23	2	0	52
		% em Encoraja-a	13,5%	38,5%	44,2%	3,8%	0,0%	100,0%
		% em HL do EE	9,1%	8,8%	16,2%	6,9%	0,0%	10,8%
Total		F	77	228	142	29	5	481
		% em	16,0%	47,4%	29,5%	6,0%	1,0%	100,0

	Encor aja-a						%
	% em HL do EE	100,0%	100,0%	100,0%	100,0 %	100,0%	100,0 %

Quadro 65- Teste qui-quadrado das variáveis frequência com que o EE encoraja a criança a explorar na *internet* e habilitações literárias

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	22,273[a]	16	,135
Razão de verossimilhança	22,073	16	,141
Associação Linear por Linear	3,538	1	,060
N de Casos Válidos	481		
a. 8 células (32,0%) esperavam uma frequência menor que 5. A frequência mínima esperada é ,54.			

Quadro 66- Frequência com que o EE sugere modos de usar a *internet* de forma segura, por habilitação literária

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Sugere modos de usar a *internet* de forma segura	Nunca	F	5	22	18	45
		% em Sugere	11,1%	48,9%	40,0%	100,0%
		% em Habilitações	6,7%	9,3%	10,2%	9,2%
	Quase nunca	F	5	11	14	30
		% em Sugere	16,7%	36,7%	46,7%	100,0%
		% em Habilitações	6,7%	4,7%	7,9%	6,1%
	Algumas vezes	F	19	55	44	118
		% em Sugere	16,1%	46,6%	37,3%	100,0%
		% em Habilitações	25,3%	23,3%	24,9%	24,2%
	Muitas vezes	F	31	79	62	172
		% em Sugere	18,0%	45,9%	36,0%	100,0%
		% em Habilitações	41,3%	33,5%	35,0%	35,2%
	Quase sempre	F	15	69	39	123
		% em Sugere	12,2%	56,1%	31,7%	100,0%
		% em Habilitações	20,0%	29,2%	22,0%	25,2%
Total		F	75	236	177	488
		% em Sugere	15,4%	48,4%	36,3%	100,0%
		% em Habilitações	100,0%	100,0%	100,0%	100,0%

Quadro 67- Teste qui-quadrado das variáveis frequência com que o EE sugere modos de usar a *internet* de forma segura e habilitações literárias

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	6,667[a]	8	,573
Razão de verossimilhança	6,700	8	,569
Associação Linear por Linear	1,020	1	,312
N de Casos Válidos	488		
a. 1 células (6,7%) esperavam uma frequência menor que 5. A frequência mínima esperada é 4,61.			

Quadro 68- Frequência com que o EE fala com a criança sobre o que ela faz *online*, por habilitação literária

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Fala com a criança sobre o que ela faz *online*	Nunca	F	6	15	6	27
		% em Fala com a criança sobre o que ela faz *online*	22,2%	55,6%	22,2%	100,0%
		% em Habilitações	8,2%	6,4%	3,4%	5,6%
	Quase nunca	F	2	3	4	9
		% em Fala com a criança sobre o que ela faz *online*	22,2%	33,3%	44,4%	100,0%
		% em Habilitações	2,7%	1,3%	2,3%	1,9%
	Algumas vezes	F	11	41	35	87
		% em Fala com a criança sobre o que ela faz *online*	12,6%	47,1%	40,2%	100,0%
		% em Habilitações	15,1%	17,4%	19,9%	18,0%
	Muitas vezes	F	30	96	71	197
		% em Fala com a criança sobre o que ela faz *online*	15,2%	48,7%	36,0%	100,0%
		% em Habilitações	41,1%	40,9%	40,3%	40,7%
	Quase sempre	F	24	80	60	164
		% em Fala com a criança sobre o que ela faz *online*	14,6%	48,8%	36,6%	100,0%
		% em Habilitações	32,9%	34,0%	34,1%	33,9%
Total		F	73	235	176	484
		% em Fala com a criança sobre o que ela faz *online*	15,1%	48,6%	36,4%	100,0%
		% em Habilitações	100,0%	100,0%	100,0%	100,0%

Quadro 69- Teste qui-quadrado das variáveis frequência com que o EE fala com a criança sobre o que ela faz *online* e habilitações literárias

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	4,338[a]	8	,825
Razão de verossimilhança	4,463	8	,813
Associação Linear por Linear	,647	1	,421
N de Casos Válidos	484		
a. 4 células (26,7%) esperavam uma frequência menor que 5. A frequência mínima esperada é 1,36.			

Quadro 70- Frequência com que o EE ajuda a criança quando algo a aborrece na *internet*, por habilitação literária

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Ajuda quando alguma coisa a aborrece na *internet*	Nunca	F	11	24	20	55
		% em Ajuda	20,0%	43,6%	36,4%	100,0%
		% em Habilitações	15,1%	10,7%	11,6%	11,7%
	Quase nunca	F	1	12	13	26
		% em Ajuda	3,8%	46,2%	50,0%	100,0%
		% em Habilitações	1,4%	5,3%	7,6%	5,5%
	Algumas vezes	F	12	46	32	90
		% em Ajuda	13,3%	51,1%	35,6%	100,0%
		% em Habilitações	16,4%	20,4%	18,6%	19,1%
	Muitas vezes	F	20	60	47	127
		% em Ajuda	15,7%	47,2%	37,0%	100,0%
		% em Habilitações	27,4%	26,7%	27,3%	27,0%
	Quase sempre	F	29	83	60	172
		% em Ajuda	16,9%	48,3%	34,9%	100,0%
		% em Habilitações	39,7%	36,9%	34,9%	36,6%
Total		F	73	225	172	470
		% em Ajuda	15,5%	47,9%	36,6%	100,0%
		% em Habilitações	100,0%	100,0%	100,0%	100,0%

Quadro 71- Teste qui-quadrado das variáveis frequência com que o EE ajuda a criança quando algo a aborrece na *internet* e habilitações literárias

Testes qui-quadrado			
	Valor	df	Significância Assintótica (Bilateral)
Qui-quadrado de Pearson	5,355[a]	8	,719
Razão de verossimilhança	6,176	8	,628
Associação Linear por Linear	,340	1	,560
N de Casos Válidos	470		
a. 1 células (6,7%) esperavam uma frequência menor que 5. A frequência mínima esperada é 4,04.			

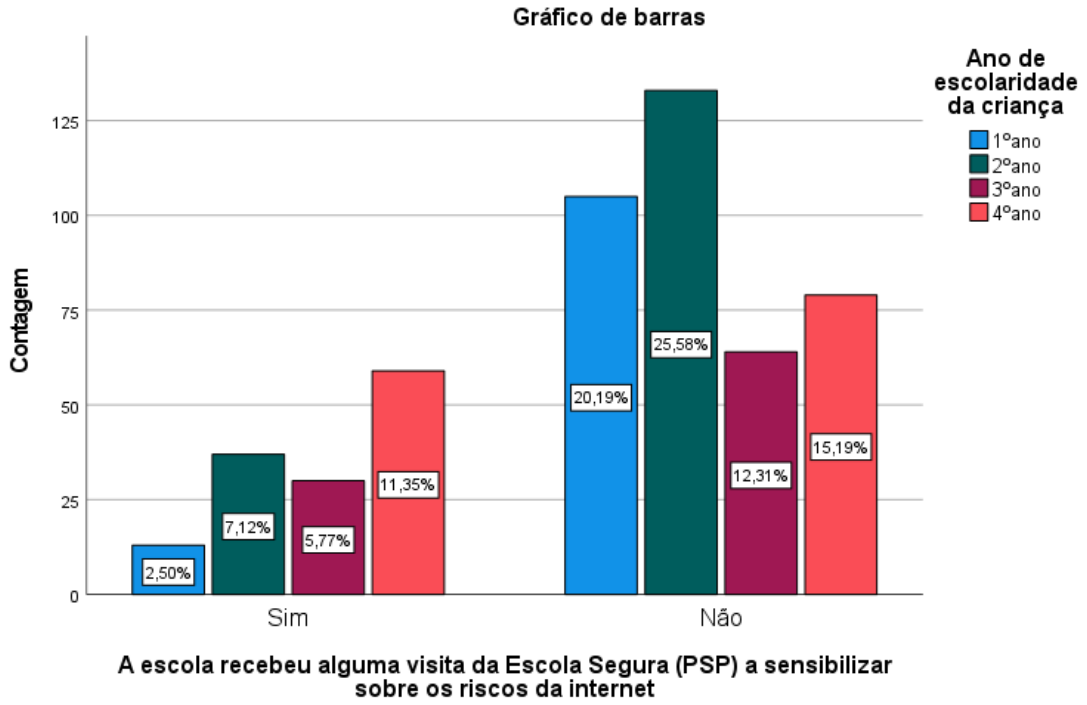


Gráfico 9- Receber visita da Escola Segura, por ano de escolaridade

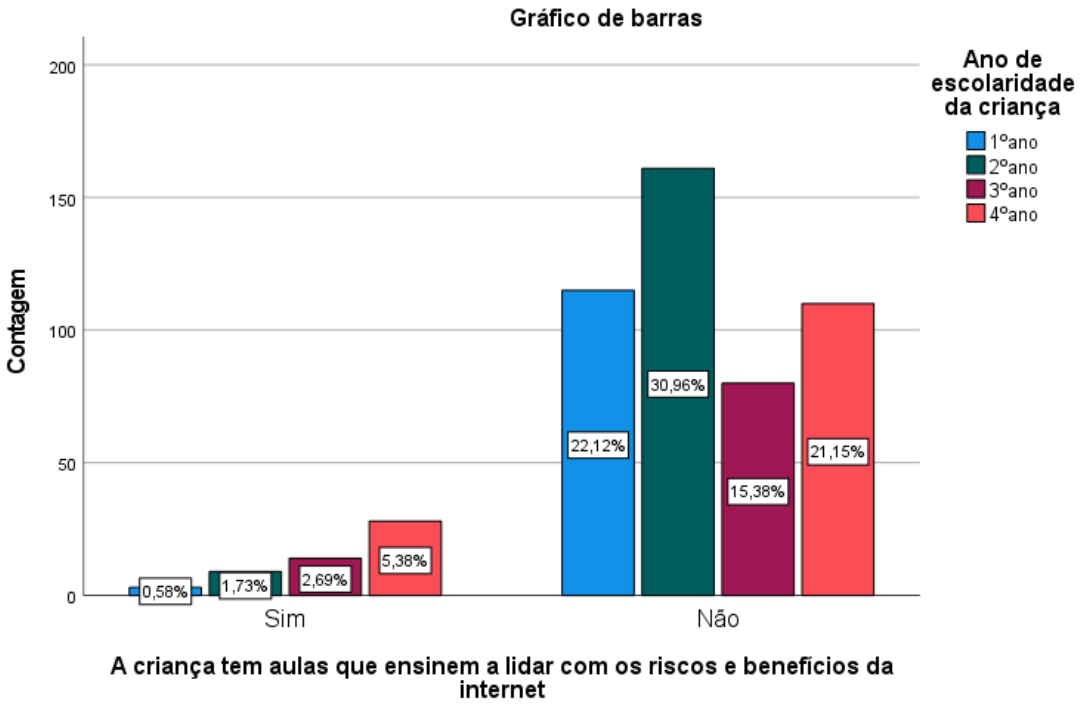


Gráfico 10- Ter aulas sobre os benefícios e riscos da *internet*, por ano de escolaridade

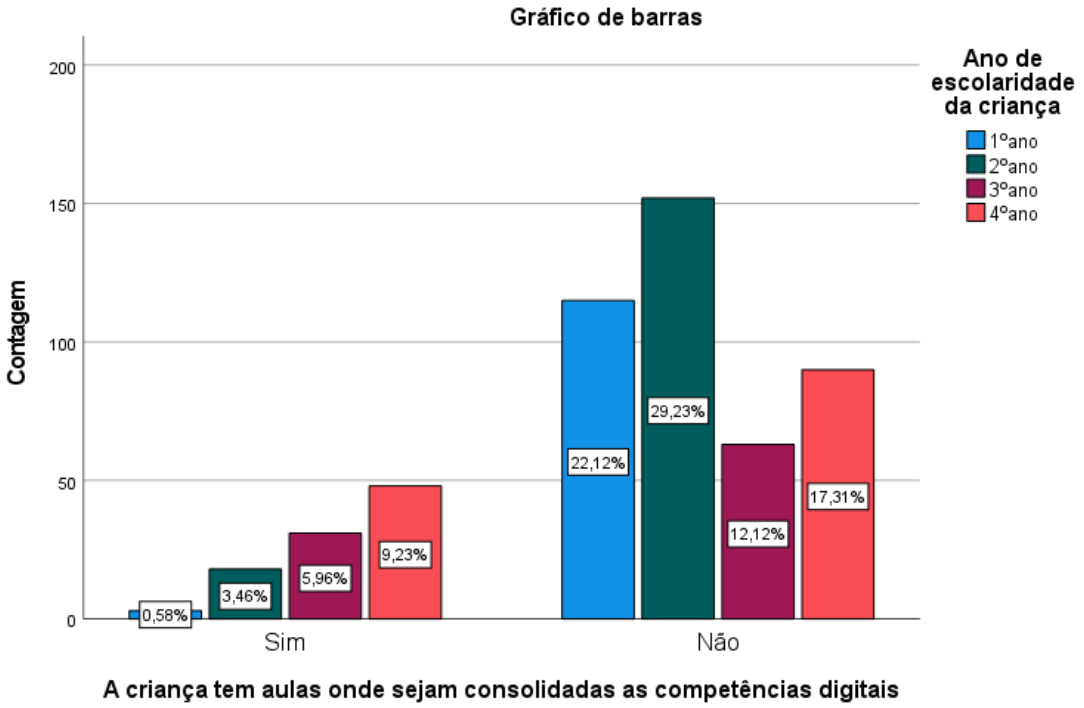


Gráfico 11- Ter aulas de competências digitais, por ano de escolaridade

Quadro 72- Comparação das escolas relativamente à ida da Escola Segura e ao leccionamento de aulas sobre os riscos da *internet* e sobre competências digitais

			Escola		Total
			Escola José Tagarro	Escola Manuel Coco	
Ida da ES à escola e leccionamento de aulas sobre riscos da *internet* e competências digitais[a]	A escola recebeu alguma visita da Escola Segura (PSP) a sensibilizar sobre os riscos da *internet*	Frequência	55	84	139
		% em $Q10	39,6%	60,4%	
		% em Escola	47,8%	83,2%	
	A criança tem aulas que ensinem a lidar com os riscos e benefícios da *internet*	Frequência	34	20	54
		% em $Q10	63,0%	37,0%	
		% em Escola	29,6%	19,8%	
	A criança tem aulas onde sejam consolidadas as competências digitais	Frequência	77	23	100
		% em $Q10	77,0%	23,0%	
		% em Escola	67,0%	22,8%	
Total		Frequência	115	101	216
Percentagens e totais têm respondentes como base.					
a. Grupo de dicotomia tabulado no valor 1.					

Quadro 73- Comparação das escolas relativamente às habilitações dos EE

			Habilitações			Total
			Ensino Básico	Ensino Secundário	Ensino Superior	
Escola	Escola Básica José Tagarro	Frequência	40	134	100	274
		% em Escola	14,6%	48,9%	36,5%	100,0%
		% em Habilitações	49,4%	53,2%	53,5%	52,7%
	Escola Básica Manuel Coco	Frequência	41	118	87	246
		% em Escola	16,7%	48,0%	35,4%	100,0%
		% em Habilitações	50,6%	46,8%	46,5%	47,3%
Total		Frequência	81	252	187	520
		% em Escola	15,6%	48,5%	36,0%	100,0%
		% em Habilitações	100,0%	100,0%	100,0%	100,0%

Quadro 74- Comparação das escolas relativamente às medidas selecionadas pelos EE a implementar

			Escola		Total
			Escola José Tagarro	Escola Manuel Coco	
Medidas a implementar na escola[a]	Mais investimento nas idas da Escola Segura à escola para falar de *cyberbullying,* violência *online,* etc.	Frequência	225	214	439
		% em $Q11_Medidas	51,3%	48,7%	
		% em Escola	86,9%	94,3%	
	Maior proximidade da Polícia com os EE (ações de sensibilização/formação)	Frequência	88	86	174
		% em $Q11_Medidas	50,6%	49,4%	
		% em Escola	34,0%	37,9%	
	Maior proximidade da Polícia com os professores e restante comunidade escolar	Frequência	103	79	182
		% em $Q11_Medidas	56,6%	43,4%	
		% em Escola	39,8%	34,8%	
	Maior investimento na formação sobre a utilização da *internet* junto dos pais	Frequência	104	75	179
		% em $Q11_Medidas	58,1%	41,9%	
		% em Escola	40,2%	33,0%	
	Deixar ficar na sala de aula os computadores emprestados pelo Ministério	Frequência	25	24	49
		% em $Q11_Medidas	51,0%	49,0%	
		% em Escola	9,7%	10,6%	
Total		Frequência	259	227	486

Percentagens e totais têm respondentes como base.

a. Grupo de dicotomia tabulado no valor 1.

Quadro 75- Comparação das escolas relativamente às atividades que as crianças mais praticam nos tempos livres

			Escola		Total
			Escola José Tagarro	Escola Manuel Coco	
Atividades mais praticadas pela criança nos tempos livres[a]	Pratica desporto ou outras atividades físicas	Frequência	141	132	273
		% em $Q3	51,6%	48,4%	
		% em Escola	54,2%	55,7%	
	Joga videojogos	Frequência	111	87	198
		% em $Q3	56,1%	43,9%	
		% em Escola	42,7%	36,7%	
	Conversa e diverte-se com amigos *online*	Frequência	36	54	90
		% em $Q3	40,0%	60,0%	
		% em Escola	13,8%	22,8%	
	Faz atividades ao ar livre	Frequência	160	141	301
		% em $Q3	53,2%	46,8%	
		% em Escola	61,5%	59,5%	
	Conversa e diverte-se com amigos cara a cara	Frequência	116	88	204
		% em $Q3	56,9%	43,1%	
		% em Escola	44,6%	37,1%	
	Ajuda a família nas tarefas domésticas	Frequência	156	147	303
		% em $Q3	51,5%	48,5%	
		% em Escola	60,0%	62,0%	
Total		Frequência	260	237	497
Percentagens e totais têm respondentes como base.					
a. Grupo de dicotomia tabulado no valor 1.					