Thiago José Ximenes Machado

A CIBERSEGURANÇA PARA ADOLESCENTES

Uma proposta para a sua comunicação

Universidade Fernando Pessoa

Porto, 2022

Thiago José Ximenes Machado

A CIBERSEGURANÇA PARA ADOLESCENTES

Uma proposta para a sua comunicação

Universidade Fernando Pessoa

Porto, 2022

A CIBERSEGURANÇA PARA ADOLESCENTES

Uma proposta para a sua comunicação

Thiago José Ximenes Machado

Tese apresentada a Universidade Fernando Pessoa como parte dos requisitos para obtenção de grau de Doutor em Ciência da Informação – Especialidade em Sistemas, Tecnologias e Gestão da Informação, orientada pelo Professor Doutor Luis Borges Gouveia

Universidade Fernando Pessoa

Porto, 2022

Resumo

Com o crescimento desenfreado das tecnologias de informação e comunicação e o uso generalizado da Internet, o mundo passou a ter mais conforto em fazer tarefas do dia-a-dia, seja no âmbito cotidiano ou profissional. Todavia, junto com essas evoluções vieram novas modalidades de crime, em especial contra aqueles que ainda são adolescentes e por essa razão possuem menor maturidade ou se encontram em fase de desenvolvimento biológico. Assim, há uma grande preocupação em comunicar e conscientizar este grupo de usuários de tecnologias, como os que por eles são responsáveis, com o objetivo de reduzir os riscos que podem afetar direta e indiretamente, e dos quais pode resultar, na maioria das vezes, em problemas psíquicos e até graves consequências à integridade física e a vida.

A relevância do estudo parte da premissa que não é encontrado com facilidade um material que contemple, em uma linguagem simples, conteúdo falando de cibercrimes e cibersegurança, especificamente para adolescentes. Assim, a nossa fonte de motivação foi justamente por atuar na segurança público do Estado, ser pai de adolescente, e a preocupação com este público vulnerável que se espalha pelo mundo. Todavia, o desafio será de colher dados, por meio de entrevistas, que possam nos levar a uma análise, de facto, sobre o conhecimento, de pais e responsáveis legais, relacionado a temática estudada nesta tese.

Partimos da metodologia de estudo voltada para análise de documentos científicos, para então iniciarmos a jornada rumo ao objetivo final. Assim, aprofundamos nosso conhecimento, escrevendo um capítulo sobre o impacto do digital no crime, para explorarmos os conceitos de cibercrimes e cibersegurança. Em seguida, documentamos um estudo sobre as ameaças e vulnerabilidades associadas aos cibercrimes com adolescente, onde adentramos no universo de pesquisa do nosso público-alvo. E finalmente, exploramos um tema atual e que está diretamente relacionado com os crimes cibernéticos. Em complemento, foram analizados os efeitos da Covid19 nas questões de cibersegurança.

Após a criação do questionário, fizemos a sua divisão em grupos, para a melhor compreensão e análise futura dos dados extraídos, inclusive se utilizando do conteúdo das questões envolvidas, para justificar as perguntas e respostas colocadas na cartilha de prevenção, que constitui o principal contributo deste trabalho.

Em continuidade da apresentação dos resultados de acordo com a divisão, por grupos, realizada no questionário aplicado, foi realizada uma análise do que for coerente e de relevância para, posteriormente, podemos elaborar um modelo de prevenção que contribua no contexto da sociedade, em especial, envolvendo os familiares e profissionais que lidam com adolescentes, e que possuem a necessidade de os orientar neste mundo digital.

Finalmente, faremos uma revisão dos objetivos traçados, comentando sobre os resultados obtidos e a contribuição da pesquisa, bem como indicações de trabalhos futuros que possam melhorar, ainda mais, está proposta de comunicação relacionada com a cibersegurança para adolescentes.

Palavras-chaves: Cibercrime; Cibersegurança; Adolescente; Internet; Tecnologias de Informação e Comunicação; Prevenção.

Abstract

With the unrestrained growth of information and communication technologies and the widespread use of the Internet, the world has become more comfortable in doing day-to-day tasks, whether in the daily or professional sphere. However, along with these developments came new types of crime, especially against those who are still adolescent and for that reason have less maturity or are in the stage of biological development. Thus, there is a great concern in communicating and raising awareness of this group of technology users, such as those responsible for them, with the aim of reducing the risks that can directly and indirectly affect, and which can result, in most cases, in problems psychic and even serious consequences to physical integrity and life.

The relevance of the study comes from the premise that it is not easy to find material that contains, in a simple language, content talking about cybercrime and cybersecurity, specifically for adolescents. Thus, our source of motivation was precisely because we work in public security in the state, being the father of an adolescent, and the concern with this vulnerable public that is spreading around the world. However, the challenge will be to collect data, by means of interviews, that can lead us to an analysis, in fact, of the knowledge, of parents and legal guardians, related to the theme studied in this thesis.

We started from a study methodology focused on the analysis of scientific documents, to then start the journey towards the final objective. Thus, we deepen our knowledge by writing a chapter on the impact of digital on crime, to explore the concepts of cybercrime and cybersecurity. Next, we document a study on the threats and vulnerabilities associated with teenage cybercrime, where we enter the research universe of our target audience. And finally, we explored a current theme that is directly related to cybercrime, so we produced a text about the effects of Covid19 on cybersecurity issues.

After creating the questionnaire, we divided it into groups, for a better understanding and future analysis of the extracted data, including using the content of the questions involved, to justify the questions and answers placed in the prevention booklet, which is the main focus of this thesis.

In continuity, we will present the results according to the division, by groups, carried out in the questionnaire applied. And, with this data in hand, we will analyze what is coherent and relevant, so that, afterwards, we can elaborate a prevention model that contributes to society, especially to family members and professionals who deal with adolescents and have the need to guide them.

Finally, we will make a review of the objectives outlined in the lighthouse of the thesis, commenting on the results obtained and the contribution of this research, as well as indications of future work that can further improve this proposal of communication related to cybersecurity for adolescents.

Keywords: Cybercrime; Cybersecurity; Adolescent; Internet; Information and Communication Technologies; Prevention.

Agradecimentos:

A Deus, força invisível, luz fortalecedora, paz imensurável, ser onipresente, onipotente e onisciente que é responsável pela minha criação e por me permitir viver a vida terrena e ter a oportunidade de evoluir, por meio do ganho de conhecimentos humanos, para auxiliar outras pessoas as quais desses necessitem. Meu Deus, não seria absolutamente nada sem sua presença em minha vida.... Muito obrigado...

A Nossa Senhora do Perpétuo Socorro, minha mãezinha dos céus, minha devoção eterna a este ser iluminado que me cobre com seu manto sagrado e me protege de todo o mal. Obrigado, minha mãezinha querida.

A São Miguel Arcanjo, meu anjo protetor, o qual está tatuado em minhas costas, protegendo a mim e a todos que amo. Obrigado, chefe do exército celestial dos anjos.

A minha mãe, ser iluminado por Deus, que dispos toda sua vida, sua liberdade, seu amor, sua dedicação, seu tempo, em prol de uma criação justa e perfeita. Obrigado por tudo, saiba que sem a senhora eu não seria absolutamente nada.

Ao meu pai, meu eterno herói, o qual palavras são insuficientes para descrever esse ser humano que foi enviado por Deus com a árdua missão de promover minha construção física, psicológica, profissional, familiar dentre outras. Obrigado por tudo, nada seria sem seus cuidados e dedicação.

A minha incasável e brilhante esposa e companheira de todas as horas, Márcia Tavares. Que Deus lhe abençoe hoje e sempre. Muita Luz e Paz em seu caminho. Obrigado por tudo.

A minha filha Maria Flor, meu maior tesouro, minha razão de viver, te amo infinitamente, minha princesinha. Obrigado por todo amor e carinho que você dar ao papai. Amor eterno!!!

A minha filha Karolina que com todo seu amor, me mostrou o verdadeiro significado da palavra pai. Obrigado por me ensinar a ser pai, a cada dia. Deus abençoe sua vida...

Ao meu orientador, Luis Borges Gouveia, que com sua sapiência me orientou de forma justa e perfeita, me ajudando a trilhar o caminho do saber rumo a realização de um grande sonho, ser doutor.

A minha irmã, mulher guerreira, dedicada, de personalidade forte, mas, de um coração gigante e que da sua maneira ama de forma incondicional os seus. Obrigado por esta ao meu lado em todos os momentos de minha vida.

Ao meu sobrinho e afilhado Andrézinho que veio a esse mundo para ensinar o verdadeiro significado da palavra Amor e que me inspira com seu notório conhecimento científico. Obrigado pelos ensinamentos e carinho com titio/padrinho.

A minha avó Zé (*in memória*), a qual sempre me enriqueceu e fortaleceu com suas maravilhosas bençãos, dizendo palavras generosas e abençoadas que me encherão eternamente de força para lutar e vencer.

A minha avó Neuda (*in memória*), ao meu avô Jacy (*in memória*) que sempre acreditaram no meu sucesso e que agora são estrelinhas que brilham no céu. Obrigado e sempre estejam presentes em meu coração.

Ao meu sogro Sinval (*in memória*) que em vida sempre confiou e acreditou no meu trabalho e nos meus conhecimentos. Obrigado, olhe por nós ai de cima.

Aos meu sogro Paulo e minha sogra Sônia, que sempre confiaram em mim para auxiliá-los e orientá-los nos mais diversos momentos de suas vidas. Obrigado pelo carinho e respeito.

A todos os membros da família Ximenes Machado que mesmo distante sempre intercedem por mim, através de orações e boas vibrações. Obrigado por fazerem parte da minha vida.

Ao meu irmão do coração e alma, Luiz Márcio Teixeira Cypriano, que com sua sapiência sempre me orienta a enfrentar as situações do cotidiano, bem como, com seus conhecimentos técnicos-jurídicos sempre esclarece minhas dúvidas e me enriquece de conteúdos normativos. Obrigado por me escolher para ser seu irmão de espírito e de coração.

A minha sobrinha Luana Menezes a qual considero meu braço direito na organização, administração e coordenação das turmas preparatórias para concursos públicos. Obrigado por existir em minha vida, gratidão pelo carinho e por toda ajuda dada, principalmente, nos momentos mais difíceis da minha vida.

A minha sobrinha Letícia, pessoa iluminada que sempre está ao meu lado me ajudando a superar os momentos complicados, bem como, compartilhando dos bons. Obrigado por ser essa sobrinha presente e amiga.

Aos meus amigos da Polícia Civil do Estado do Pará, Polícia Militar do Estado do Pará, Detran do Estado do Pará, Polícia Federal, Guarda Municipal de Belém, SEAP do Estado do Pará, Corpo de Bombeiros Militar do Estado do Pará, Centro de Perícia Renato Chaves do Estado do Pará, SEMOB da cidade de Belém do Estado do Pará, que estão sempre tecendo elogios, assim como, incentivando a minha carreira educacional e jurídica. Obrigado pelo apoio dado nas horas mais difíceis da vida.

Ao amigo, padrinho e professor de língua portuguesa, Lobão, que com seu extraordinário domínio da ortografia e gramática fez a brilhante correção desta tese. Obrigado por contribuir com está nobre obra.

Aos meus animais Pérola, Tilió, Pangaré (*in memória*), Foe (*in memória*), Lili (*in memória*), Zeus (*in memória*), Belinha (*in memória*) e aos peixinhos que abrilhantam a nossa casa, gerando um ambiente de Paz e contato direto com a natureza. Obrigado por trazer tranquilidade para meu lar.

Aos meus amigos e professores portugueses que me acolheram com muita hospitalidade em seu país, durante os períodos de estudo no mestrado e, atualmente, no doutorado. Obrigado por me presentearem com uma segunda pátria.

Ao médico e amigo Dr. Guilherme Soares que consegue promover meu equilíbrio químico para que eu possa produzir obras como esta. Obrigado que Deus lhe sabedoria para ajudar seus pacientes.

A minha psicóloga Elinete Muniz que com seu vasto conhecimento me ajudar a equilibrar meu psicológico. Obrigado por me manter estabilizado psicologicamente e a fazer eu conhecer meus traços e gatilhos.

GRATIDÃO À TODOS!!!

Índice

CAPÍTULO 1

CAPÍTULO 2

Impacto do digital no crime

CAPÍTULO 3

Ameaças e vulnerabilidades associadas aos cibercrimes com adolescentes

CAPÍTULO 4

Os efeitos da covid19 nas questões de cibersegurança

CAPÍTULO 5

Metodologia

CAPÍTULO 6

Proposta de um modelo que possa auxiliar os pais, os professores, o Estado e até mesmo o próprio adolescente, a reduzir os riscos cibernéticos

CAPÍTULO 7

Resultados da aplicação oficial do questionário

CAPÍTULO 8

Análises

APÊNDICES

ANEXOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ABREVIATURAS

E.C.A – Estatuto da Criança e do Adolescente.

IBGE – Instituto Brasileiro de Geografia e Estatística.

PNAD – Pesquisa Nacional por Amostra de Domicílios.

NIST – Instituto Internacional de Padrão de Tecnologia.

ITU – União Internacional de Telecomunicações.

HIV - Vírus da Imunodeficiência Humana.

IoT – Internet das Coisas.

OAE – Organização dos Estados Americanos.

IIN – Instituto Interamericano da Criança.

COVID – Doença do Coronavírus.

OMS – Organização Mundial de Saúde).

VPN – Rede Virtual Privada.

URL – Localização Uniforme de Recursos (endereço de site).

CAPÍTULO 1

1.1 – Introdução

O capítulo 1 da tese de doutoramento, mostrará o contexto e relevância do tema abordado, trazendo primeiramente a faixa etária que compreende o público adolescente, segundo o Estatuto da Criança e do Adolescente, bem como as principais caraterísticas desta fase evolutiva de nossas vidas. Em seguida, traremos a motivação para realização da pesquisa com tema relacionado a cibersegurança e cibercrimes voltados para o público mencionado anteriormente. Continuaremos, com os problemas e desafios que iremos enfrentar para este estudo tão importante e de relevância mundial. Logo em seguida, apresentaremos, os objetivos da realização da pesquisa, o objeto e os limites, já que estamos diante de ciberespaço, isto é, um imenso universo. E, finalmente, será apresentado a estrutura para o trabalho de pesquisa ser realizado com organização, importância e coerência de informações.

Iniciaremos nossa jornada, pelo mundo do cibercrime e da cibersegurança, trazendo o impacto do digital no crime, o qual abordaremos a evolução da rede mundial de computadores e chegaremos ao tão atual conceito de sociedade da informação. Em sequência, mostraremos o desenvolvimento dessa era digital, falando da cloud à Internet das coisas. Então, adentraremos o conceito de cibercrimes, suas espécies e as alterações e modificações realizadas no Estatuto da Criança e do Adolescente, ligada a este tema. Passaremos pela inserção de novas modalidades de crimes informáticos no código penal brasileiro, e em seguida uma breve reflexão sobre as penas aplicadas a estes delitos. Ainda capítulo 2, entenderemos o que é a sociedade digital, os conceitos de cibersegurança e a criminalidade facilitada pela era tecnológica. Então, começaremos a envolver os nossos principais protagonistas da tese, isto é, o adolescente, e falaremos sobre as mudanças em suas vidas com essa era informatizada.

No capítulo 3, traremos a temática relacionada as ameaças e vulnerabilidades associadas aos cibercrimes com adolescente. Neste contexto, disponibilizaremos informações relacionadas as características comportamentais dos adolescentes que favorecem a sua vulnerabilidade, e em seguida, falaremos de facto sobre a vulnerabilidade dos adolescentes e quais as ameaças cibernéticas que cercam estes. Achamos importante descrever os aspectos de convivência entre os adolescentes, seus responsáveis e a sociedade contemporânea, e com base nessas

informações traremos os riscos os quais as ameaças de cibercrimes podem se concretizarem, tendo em vista esta vulnerabilidade apontada aos adolescentes. Ressaltaremos ainda, o importante papel dos pais e responsáveis legais na prevenção desses tipos de delitos, e acabamos por expandir a temática mostrando aos professores e educadores a importância de tratar sobre o tema de cibercrimes e cibersegurança dentro das salas de aula, bem como o papel da mídia em propagar esse assunto. Finalizamos, com uma reflexão sobre os cuidados do acesso à Internet feito por adolescentes.

Com nosso atual cenário pandêmico, resolvemos desenvolver, no capítulo 4, uma associação deste com o tema tratado na nossa tese, e então desenvolvemos a temática sobre os efeitos da Covid19 nas questões de cibersegurança. Então, partimos dos comentários acerca do uso das tecnologias associadas à Internet em tempos de pandemia, pois sabemos o quanto ficamos dependentes desta, já que passamos por isolamentos e *lockdowns*. Logo, diante deste cenário, verificaremos a grande oportunidade dos cibercriminosos praticarem seus delitos, em especial quando se trata de pessoas que tiveram que passar suas tarefas para o modo *home office*, porém, não tem *expertise* de segurança tecnológica, a qual, em regra, era fornecida por suas empresas. Ainda ressaltaremos, a situação das crianças e dos adolescentes diante ao maior tempo de acesso à Internet em época de pandemia. E neste contexto geral, importante trazermos um breve estudo de vitimologia, isto é, levando em consideração a participação ou não das vítimas de cibercrimes. E, por fim, mostraremos um pequeno protocolo de segurança, o qual pode ser seguido para minimizar as possibilidades de cairmos nas garras desses criminosos.

No capítulo 5, traremos a metodologia utilizada para desenvolver a tese, onde iniciamos falando sobre a abordagem metodológica qualitativa da investigação, já que esta foi a escolhida por nós para realização da pesquisa, que por sinal, se trata do tipo documental, tendo em mente que reuniremos vários documentos científicos para nos embasar no decorrer de todo o trabalho. Em seguida, discorreremos do método de recolha de dados e análise do questionário que será aplicado aos participantes, isto é, pais ou responsáveis legais dos adolescentes, e consequentemente iremos justificar o motivo da escolha destes participantes. Logo após, mostraremos a divisão que foi realizada para melhor organizar nossa pesquisa, isto é, dividiremos em grupos, que são: identificação, conectividade, caracterização, hábitos digitais e consciência. E, para findar, apresentaremos na íntegra o questionário que será formulado e distribuídos para serem preenchidos, e como forma de justificativa, esclareceremos o porquê da escolha de tais perguntas.

A proposta de um modelo que possa auxiliar os pais, os professores, o estado e até mesmo o próprio adolescente, a reduzir os riscos cibernéticos será apresentada no capítulo 6, onde apresentaremos os modelos existentes em alguns sites que tratam do assunto de segurança cibernética, enfatizando que apenas trazem os conceitos e prevenções sobre vírus e malwares, de uma forma bastante genérica. Em seguida, traremos o processo construtivo e o próprio modelo de prevenção de cibercrimes, mais especificamente, contra adolescentes. Ainda exibiremos as formas de comunicar tal assunto relacionado a estas espécies de delito. E, para finalizar, apresentaremos o nosso manual para auxiliar adolescentes sobre os cibercrimes e cibersegurança, contendo 30 (trinta) perguntas e suas respectivas respostas, de forma simples e de fácil entendimento.

O capítulo 7, foi reservado para mostrarmos os resultados da aplicação oficial do questionário, trazendo informações que perpassam pelas instruções dadas antes de iniciar o preenchimento deste até os valores reais, e, em percentagem, dos resultados obtidos em cada pergunta feita, após ser aplicado para 200 (duzentos) participantes. Vale ressaltar, que dividiremos em grupos para que haja uma melhor compreensão do leitor, além de exibirmos gráficos, onde a visualização dos dados ficam mais compreensíveis. E, para finalizar, falaremos do modo utilizado para fazer a recolha dos dados, bem como o instrumento usado para tal.

O penúltimo capítulo, que é o oitavo, vai tratar das análises dos dados relacionados à cibersegurança, que foram colhidos e colocados em uma planilha eletrônica para melhor poderem ser trabalhados. Esta análise, será feita por grupos, conforme foi dividido nosso questionário, apresentando os valores percentuais, em tabelas e gráficos, do cruzamento de dados os quais foram considerados relevantes e coerentes. Em seguida faremos um quadro de resumo com o essencial da análise por grupos de questões, para que seja mais bem visualizado e compreendido. E com intuito de aprofundar a análise, mostraremos algumas considerações adicionais, onde serão cruzados os dados dos diversos grupos, especificando, inclusive, informações relacionadas dos adolescentes do sexo masculino e feminino, separadamente. Após, iremos confrontar as perguntas do questionário aplicado com o manual criado para prevenção de cibercrimes, trazendo explicações do porquê o conteúdo do manual se fez importante. Esta informação é confrontada com dados estatístico da cidade de Belém do Pará, a qual foi escolhida para ser o local da colheita de dados da pesquisa, e acrescentaremos, ainda, a estratégia do governo brasileiro relacionada com a segurança da informação, bem como a sensibilidade por parte do governo do município em estudo. Para finalizar, mostramos os dados

relacionado ao acesso à Internet feito por adolescentes em Portugal, para assim, termos uma melhor visão do comportamento destes ao navegarem pelo ciberespaço.

O último capítulo mostrará os resultados obtidos, e a demonstração do quão importante, para pais e responsáveis legais, foi a realização desta pesquisa científica, tendo em vista a prova concreta da vulnerabilidade dos adolescentes ao acessarem a rede mundial de computadores. E finalmente, podemos deixar uma proposta de trabalhos futuros, os quais podem trazer maneiras, cada vez mais completa, de divulgar um conteúdo amplo e primordial para servir de orientação e prevenção contra os cibercrimes, isto é, apresentando recursos relacionados a cibersegurança.

1. 2 – Contexto e Relevância

O estudo será realizado com os adolescentes que de acordo com as regras estabelecidas pelo Estatuto da Criança e do Adolescente (ECA), que, em seu artigo 2º, estabelece o conceito de adolescente (Brasil, 2018),

> Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.

Ressaltando, que ao completar 12 anos de idade a criança já passa a ser considerada adolescente, e esta vai até os 17 anos, isto é, no dia de aniversário de 18 anos, o adolescente já passar a ser considerado adulto, por isso, imputável, podendo ser responsabilizado pelas suas atitudes em âmbito criminal.

A etapa de transição da fase infantil para adolescência é marcada por diversas transformações, tanto no que diz respeito aos aspectos físicos como psicológicos, tornando a vulnerabilidade mais exposta ao mundo virtual.

A relevância de abordamos esta faixa etária cronológica, e que nesta fase da vida surgem vários comportamentos os quais são característicos e que facilitam a ação dos cibercriminosos, tendo em vista que há uma espécie de padrão comportamental dos adolescentes, seja no Brasil ou em qualquer outros país.

Neste primeiro momento, se faz necessário mostrar essas principais características, para a posteriori definir e detalhar cada uma, fazendo sempre associação com o foco principal da tese, que é demonstrar a vulnerabilidade, para só então propor o modelo de prevenção contra os cibercrimes, isto é, a cibersegurança para adolescentes.

As principais características dos adolescentes, ao entrarem nesta nova fase de suas vidas são (Morgado, 2016):

- Agressividade/Psicoticismo – Personalidade marcada pela hostilidade e agressividade nas relações interpessoais;
- Mentiras – Tendência de esconder a verdade;
- Autoafirmação/Autocontrole – Acredita que já tem capacidade de encarrar os conflitos da vida;
- Abertura a experiências – Se envolvem em situação par experimentar e viver experiências, muitas vezes negativas;
- Neuroticismo – São fortes candidatos a problemas como depressão, ansiedade e outros;
- Aceitação social – Fazem o que for necessário para ser aceitos pela sociedade na qual está incluída;
- Empatia – Tende a se colocar no lugar de outros e tomar as suas dores, sendo defensores de causas como direitos humanos, feminismo, antirracismo, partidários e outros;
- Extroversão – Se sente bem em interagir com outros, se mostrando falante, sociável, entusiasmado, entre outras características similares.

Podemos inferir, que tais características mostrada por meio de estudos científicos são de suma importância para uma análise mais aprofundada, com objetivo de associar tais comportamentos com a vulnerabilidade relacionada a potenciais vítimas de cibercrimes.

1.2 – Motivação para o trabalho

A realização deste trabalho de pesquisa para formulação de uma tese de doutoramento, teve como ponto de partida algumas motivações concretas, as quais são expostas a seguir:

- Uma preocupação, no que diz respeito à segurança de adolescentes que se conectam à rede mundial de computadores sem que tenham a maturidade de perceber a má intenção dos algozes, os quais se utilizam dos meios virtuais para praticar delitos cruéis contra estes que estão em fase de formação biológica e psicológica;

- Aproveitar os conhecimentos adquiridos, ao longo dos anos, nas duas áreas de formação: tecnológica e direito. Promovendo assim uma verdadeira ligação no que diz respeito aos delitos praticados por meios eletrônicos, recorrendo ao conhecimento de informática e ao uso das leis para minimizar o número de vítimas adolescentes dos chamados cibercrimes;

- Decorrente da atividade laboral desenvolvida no dia-a-dia pelo investigador por fazer parte de um órgão vinculado à segurança pública e, neste contexto, tomar conhecimento de vários casos onde adolescente são vítimas dos mais perversos delitos, como crimes contra dignidade sexual de adolescentes, cyberbullying, cyberstalking, dentre outros;

- E por último, pelo facto de ser pai de duas meninas, uma ainda criança e outra recém-entrada na fase adolescente. Assim, a preocupação com o uso indevido das tecnologias é real e deve ser tratado com serenidade, porém, é necessário ter conhecimento de causa para tal.

1.3 – Problemas e desafios

Em face da velocidade na qual vem crescendo os meios de comunicação digital, em especial o acesso à rede mundial de computadores, popularmente conhecida como Internet, decorre uma necessidade de adaptação às facilidades obtidas e ao seu impacto. Precisamente, no âmbito do seu impacto, existem problemas, entre os quais estão as novas modalidades de crimes, que ficaram conhecidas como cibercrimes, resultantes de ameaças ciber. Estes podem ser classificados como próprios ou impróprios, mas é certo que ambos trazem graves complicações para as suas vítimas, ainda mais se tratando de um público mais vulnerável – os adolescentes.

A problemática a ser tratada nesta investigação diz respeito aos delitos informáticos impróprios, que são aqueles que se utilizam da tecnologia como um meio para a prática de crimes. Tendo como foco principal, o público que consideramos vulnerável, já que se encontram em fase de amadurecimento biológico e pessoal (adolescentes).

A cada ano o índice de adolescentes, vítimas dos mais variados crimes, como pedofilia infantil, pornografia voltadas à adolescentes, cyberbullying, delitos contra honra, conta a vida, entre outros, vem aumentando significativamente, já que os recursos tecnológicos fazem parte da vida destes, e que não existe, na maioria das vezes, um controle no acesso às ferramentas utilizadas na Internet.

O problema que será alvo de uma discussão aprofundada incide sobre um fenômeno que atinge as famílias do mundo inteiro. Porém, o seu estudo será limitado às ocorrências na população adolescente que possui características próprias. Existe, claro, a consciência que o problema é mais complexo e alargado a todas as faixas etárias e em se tratando de ferramentas virtuais, com uma abrangência de ordem mundial desses delitos.

Como desafio teremos que criar um modelo o qual consiga ser eficiente e eficaz na comunicação e prevenção dos mais variados cibercrimes praticados contra adolescentes. Tais orientações deverão ser aptas a servir de manual, tanto para pais e responsáveis, para professores e educadores, para implementação de políticas públicas de divulgação, assim como para o próprio público na qual a tese tem sua proposta.

1.5 – Objetivos da pesquisa

Os objetivos da presente pesquisa de doutoramento são:

- Explicitar e desenvolver um modelo de despiste que identifique o potencial de um adolescente tomar comportamentos de risco no contexto de digital;
- Definir e aprofundar os conceitos de cibercrime, cibersegurança, ameaças ciber e comportamentos de risco em adolescentes;
- Organizar as dimensões de um modelo de comportamento de risco associado com as práticas digitais de adolescentes;
- Propor um modelo de comunicação para prevenção e cibersegurança para adolescentes.

1.6 – Objeto e limite da pesquisa

O objeto da pesquisa são as ameaças ciber. Assim, o trabalho toma por base a análise e o aprofundamento de uma proposta de comunicação para adolescentes poder lidar com as ameaças ciber, no âmbito da cibersegurança.

O limite da pesquisa está associado com a própria amostra dos principais e essenciais cuidados, os quais devem ser tomados para evitar que adolescentes possam se tornar vítimas em potencial dos mais variados delitos cometidos no ciberespaço. É importante salientar que estamos no contexto de um mundo digital, emergente e sem fronteiras e com crescimento e evolução significativa e difícil de prever.

No final do trabalho, queremos ter a certeza de que o contributo é relevante, não somente para o público-alvo deste trabalho, mas para os que direto ou indiretamente os rodeiam, como pais, responsáveis, professores, poder público e outros, cada um dentro das suas atribuições e limitações e que estão implicados no processo de cibersegurança de adolescentes.

1.7 – Estrutura para o trabalho

O trabalho foi estruturado em 9 (nove) capítulos, os quais, inicialmente, começam a explorar os assuntos relacionados a cibercrime e cibersegurança, e após envolvidos com o tema, passam a aprofundar o estudo, de forma mais específica, focando no nosso objeto de pesquisa, tomando o público escolhido para trabalhar: os adolescentes. Assim, a estrutura foi construída da seguinte maneira:

- Capítulo 1 – Mostra de modo geral quais as características, relevância, motivação, problemas, desafios, objetivos e limites da pesquisa científica que escolhemos para construção do trabalho aqui reportado;
- Capítulo 2 – É discutido o impacto do digital no crime, onde abordamos os conceitos básicos de Internet, evolução da rede mundial de computadores e os seus serviços, cibercrimes, conteúdo da lei penal brasileira relacionadas a delito cibernéticos, sociedade digital e cibersegurança, com ênfase na proteção dos adolescentes;
- Capítulo 3 – É apresentada a temática sobre ameaças e vulnerabilidades associadas aos cibercrimes com adolescentes, onde mostramos o motivo de os adolescentes serem considerados vulneráveis, incluindo aspectos psicológicos e sociais, e ainda incluímos a importância de pais, responsáveis legais, mídia, professores e educadores na divulgação e na orientação para prevenção desses cibercrimes contra este grupo de pessoas;
- Capítulo 4 – Com atual cenário que o mundo enfrenta, são realizadas discussões dos efeitos da Covid-19 nas questões de cibersegurança, e são mostrados os perigos que a tecnologia pode trazer para aqueles que não tem *expertise* suficiente, isto é, vítimas em potencial, e que não conhecem os conceitos básicos de cibersegurança. Ainda mais, tendo em consideração o aumento do uso da tecnologia, que ocorreu em decorrência do isolamento social;
- Capítulo 5 – Abordamos a metodologia utilizada para construção da tese, onde são apresentados os conceitos dos recursos utilizados no decorrer da construção e da pesquisa cientifica do trabalho em comento, justificando o motivo pelo qual foi utilizado cada ferramenta metodológica, incluindo a aplicação de um questionário como forma de recolha de dados;

- Capítulo 6 – Foi apresentado um modelo, no formato de cartilha informativa, que traz conceitos e orientações necessárias para reduzir a possibilidade do adolescente ser vitimizado por um cibercriminoso;
- Capítulo 7 – Apresentamos os resultados obtidos após a recolha de dados, criamos tabelas e apresentamos gráficos para melhor entendimento. Vale ressaltar, que organizamos os dados recolhidos em grupos para melhor trabalhar com os valores e para facilitar o cruzamento dos dados entre os diferentes grupos, representantes das dimensões a considerar;
- Capítulo 8 – Dedicamos este capítulo para realizar a análise dos dados que foram extraídos após a aplicação do questionário. Tal análise foi feita em grupos individualmente, e a combinação de dados cruzados dos grupos. Vale ressaltar, que foram analisados dados gerais do município onde foi realizada a pesquisa, bem como as estratégias para propagar o conteúdo proposto nesta tese. E, finalmente, recolhemos os dados relacionados ao acesso à Internet em Portugal, feito pelos adolescentes, para melhor visualizarmos o comportamento destes em outro país e assim comparar os resultados obtidos.
- Capítulo 9 – No último capítulo será realizada a conclusão da pesquisa, onde falaremos dos resultados obtidos, bem como da contribuição que nossa pesquisa trouxe para sociedade e de trabalhos futuros que poderão ser feitos, dando continuidade a este estudo, num tema bem atual e que ainda é carente de conteúdo simples e de fácil acesso para os que possuem menos familiaridade com o assunto relacionado a cibercrimes e cibersegurança.

CAPÍTULO 2

Impacto do digital no crime

2.1 – Introdução

Na atualidade, verificamos o veloz e crescente desenvolvimento e o uso das tecnologias que invadiram a nossa vida de forma que nos tornaram cada vez mais dependentes, já que estas nos trazem conforto e praticidade para desenvolver as nossas atividades laborais e pessoais e a um custo e esforço menor.

Em um primeiro momento, mostraremos um breve histórico sobre a evolução da Internet, que passou a ser acompanhada de uma nova interatividade entre as pessoas, denominada sociedade da informação, e que se utiliza de ferramentas tecnológicas para expandir a sua forma de comunicação, fazendo assim com que as fronteiras longínquas que separavam as pessoas fossem encurtadas, desenvolvendo o conceito de globalização.

Em seguida, apresentaremos a evolução digital, partindo do novo conceito de computação em nuvens à Internet das coisas, no qual o primeiro veio a trazer recursos que garante a economia e disponibilizam maior capacidade de armazenamento de dados, e o segundo, o qual revolucionou a maneira de interação entre os objetos e a rede mundial de computadores, ganhando espaço nos lares e no ambiente de trabalho das pessoas.

Em face de toda esta explosão tecnológica, falaremos do lado perigoso do ambiente virtual chamado de ciberespaço. Abordando os cibercrimes, tanto os que usam a Internet e os sistemas informáticos como ferramentas para prática de crimes, quanto os que nasceram em decorrência das tecnologias. Nesse mesmo raciocínio, traremos as alterações e inserções que modificaram o Estatuto da Criança e do Adolescente por meio da Lei 11.829/08, assim como a modificação do código penal brasileiro. Ao final faremos uma breve reflexão sobre as penas aplicadas para cibercrimes no Brasil.

Falaremos, em seguida, da união dessa sociedade digital e o seu casamento com a Internet das coisas, em paralelo com o surgir da denominada sociedade digital, na qual as

pessoas têm dependência da utilização dessas tecnologias para desempenhar as suas atividades diárias, seja no âmbito pessoal ou profissional. Incluiremos também os conceitos relacionados à cibersegurança, à criminalidade facilitada pela era digital, bem como, a mudança na vida dos adolescentes com o uso de dispositivos informáticos.

Finalmente, traremos um breve resumo dos principais conteúdos abordados neste trabalho de pesquisa científica.

2.2 – Evolução da Internet e sociedade da informação

Em meados da década 80, surge a rede mundial de computadores que iria, a partir de então, alavancar a globalização e o modo de viver da sociedade, que ganhara uma nova e poderosa ferramenta de comunicação, que encurtaria, virtualmente, os mais remotos povos que habitam o planeta terra.

A popularidade e a utilização da Internet explodiram, principalmente, quando foram lançados os smartphones, que na atualidade são responsáveis pelo maior número de acessos. De acordo com o site oficial de notícias do IBGE (Instituto Brasileiro de Geografia e Estatística), entre os usuários de Internet que possuem idades acima de 10 anos, 94,6% se conectaram por meio de celular. E essa conexão é em cerca de 95%, utilizada para troca de mensagens, utilizando aplicativos diferentes de e-mail, 76,4% para assistir a séries e filmes, seguido de 73,3% que fazem chamadas de vídeo e de voz, e, finalizando com 69,3% dos que se servem da comunicação por e-mail, conforme mostra o gráfico a seguir (PNAD, 2018).

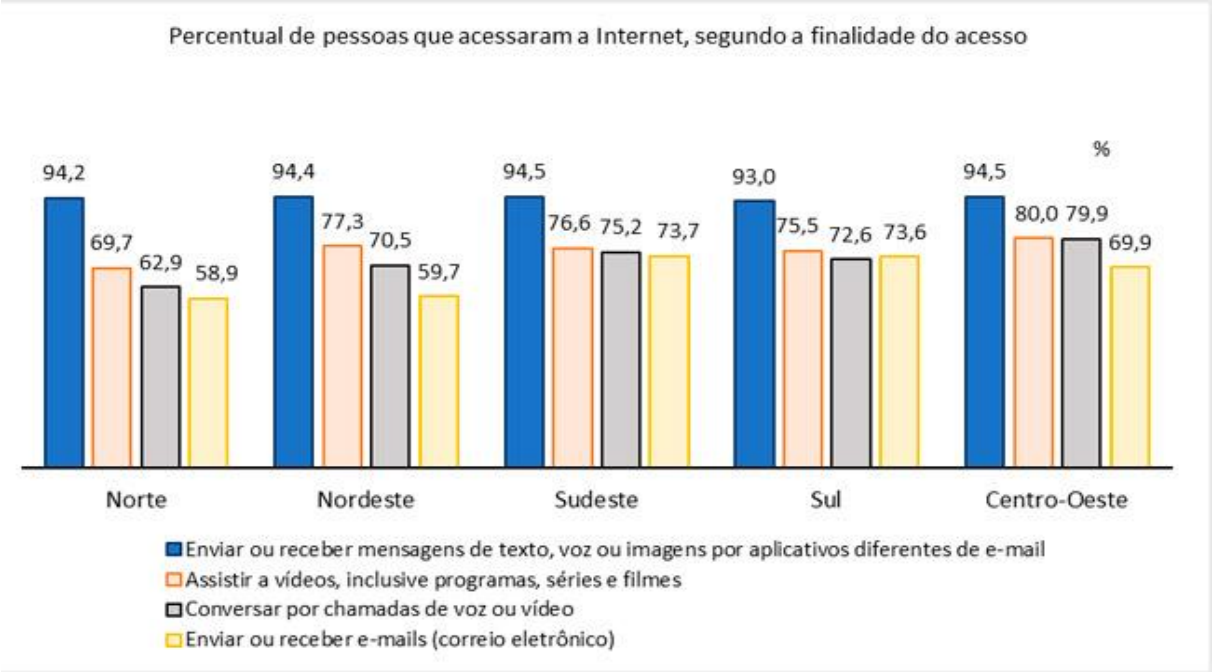


Figura 1 - Gráfico de acesso à Internet versus finalidade

Ainda de acordo com IBGE (2018), pesquisas foram realizadas no sentindo de obter dados relacionados às áreas que utilizam a Internet para melhor exercer suas atividades laborais, e ficou constado que,

> Na comparação por grupamentos das 11 atividades, o acesso à Internet foi mais elevado, nos da informação, comunicação e atividades financeiras, imobiliárias, profissionais e administrativas (92,0%), da educação, saúde humana e serviços sociais (91,2%), da administração pública, defesa e seguridade social (88,3%) e de outros serviços (87,6%). Agricultura, pecuária, produção florestal, pesca e aquicultura (28,3%) foi o grupamento de atividade com menos uso da Internet (IBGE, 2018).

Com tal surgimento e com a facilidade encontrada, o conceito de informação, veio junto a uma problemática, que é apresentada por Lancaster (Lancaster, 1989), o qual afirma que

> Informação é uma palavra usada com frequência no linguajar quotidiano e a maior parte das pessoas que a usam pensam que sabem o que ela significa. No entanto, é extremamente difícil definir informação, e até mesmo obter consenso sobre como deveria ser definida. O facto é, naturalmente, que informação significa coisas diferentes para pessoas diferentes (Lancaster, 1989).

Na atual conjuntura que se encontra a tecnologia, em especial, as diretamente relacionadas com a informação e a comunicação, vêm sendo a cada dia mais comuns e em uso entre as pessoas, que estão cada vez mais confiantes e dependentes desta era do digital.

O avanço da tecnologia, no século XX, gerou um grande impacto no cotidiano da população, abrangendo todas as áreas e atividades essenciais, tornando esta, de certa forma, dependente desses meios de informação e comunicação. Tal fenômeno contribuiu para o surgimento do conceito de sociedade da informação, conforme defendido por Luis Borges Gouveia (Gouveia, 2004),

> A Sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios electrónicos, como a rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, económicos e políticos, criando uma nova comunidade local e global: a Sociedade da Informação (Gouveia, 2004).

Por outro lado, temos a existência de habilidades diferentes, no sentido de dominar as tecnologias, tendo em vista que, em cada sociedade, esta mudança ocorre de forma desigual, inclusive relacionada ao processo temporal, e ainda levando em consideração as diferentes culturas de comunicação (Kohn, 2007). Muitas vezes, essas habilidades não vem acompanhadas do conhecimento e das atitudes certas que em conjunto com as habilidades, formam as competências – existe assim, um desiquilíbrio.

Muito importante ressaltar que, apesar da evolução de uma sociedade tradicional para uma sociedade da informação, temos que enfrentar o aparecimento dos chamados analfabetos digitais, que estão cada vez mais excluídos do mercado de trabalho, gerando assim um índice elevado de desemprego e de trabalhos informais, o que, muitas vezes, poderá refletir na prática de delitos.

Podemos perceber que a evolução crescente da Internet acaba por se confundir com o novo paradigma da sociedade da informação, uma vez que os recursos são comuns e explorados de forma intensiva na nossa sociedade.

2.3 – Desenvolvimentos recentes: da cloud à Internet das coisas

Inicialmente, é importante entendermos o conceito que vem revolucionando muitos serviços, que antes se fazia necessário possuir uma infraestrutura robusta e de alto custo para ser mantida. Esta nova infraestrutura, mais eficiente e de mais fácil manutenção é a computação em nuvem, ou no inglês *cloud computer*. A sua definição, de acordo com *National Institute of Standards and Tecnology* (NIST, 2020) é

> um modelo que possibilita acesso, de modo conveniente e sob demanda, a um conjunto de recursos computacionais configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser rapidamente adquiridos e liberados com mínimo esforço gerencial ou interação com o provedor de serviços (NIST, 2020).

Com tal inovação no campo das tecnologias de informação, a computação em nuvem trouxe uma gama de benefícios, dos quais podemos citar: o provedor que será responsável por deter e gerar todos os recursos (servidores/hardware, aplicações, armazenamento e outros); o aumento de recursos poderá ser realizado pelos usuários de forma rápida e fácil; o custo será de acordo com a utilização dos serviços; facilidade de acessar os serviços a qualquer hora e em qualquer lugar, e ainda utilizando qualquer plataforma; dentre outras vantagens (Medeiros, 2017).

Em se tratando do uso da tecnologia citada anteriormente, temos que lembrar dos usuários sem muitos conhecimentos informáticos, os quais passaram a usufruir de recursos como armazenamento em nuvem, e até mesmo utilização de aplicativos sem a necessidade de instalação no computador pessoal. E muitos desses serviços são disponibilizados de forma gratuita, como por exemplo, *icloud, google drive*, entre muitos outros.

Como toda nova tecnologia, a computação em nuvem traz algumas vulnerabilidades que devem ser levadas em consideração, partindo da premissa onde os seus dados estarão armazenados e circulando na Internet. Assim sendo, podemos ressaltar alguns problemas associados a esta nova ferramenta, que são: a possibilidade de perda ou vazamento de dados; a possibilidade de empregados da empresa provedora subtraírem ou repassarem dados; caso não haja uma boa autenticidade, as informações podem ser desviadas para outras pessoas; por

possuírem um imensurável armazenamento de dados, serão alvo dos cibercriminosos; dentre outros.

Em uma contínua evolução tecnológica, atualmente, muito se ouve falar em IoT (*Internet of Things*), que em português significa Internet das coisas, que diz respeito a um crescente e evoluído número de dispositivos, que vão desde os computadores e os *smartphones* até sensores e *chips*, os quais se conectam à Internet e são capazes de realizar comunicações com outros tipos de equipamentos, tendo como grande diferencial a ausência de intervenção humana (Unic, 2016).

De acordo com a União Internacional de Telecomunicações (ITU, do inglês *International Telecommunication Union*) a definição de IoT é "*Uma infraestrutura global para a sociedade da informação, permitindo serviços avançados através da interconexão (física e virtual) de coisas baseadas em tecnologias interoperáveis de informação e de comunicação, existentes e em evolução*" (ITU, 2012).

Percebemos que a buscar por maior conforto e comodidade, seja com um simples sensor que detecte a temperatura externa e regule o ar-condicionado para um ambiente agradável, até uma UCI (Unidade de Cuidados Intensivos) montada dentro de casa, porém monitorado por médicos de um hospital e, por muitas vezes, controlada por eles. E tudo isso, vem sendo possibilitado no contexto de uma sociedade moderna e dominada pelos recursos tecnológicos.

Por outro lado, ambientes informatizados despertaram a mente de criminosos que utilizam ferramentas virtuais, e que se aproveitam dos usuários sem conhecimentos necessários para manusear de forma segura os dispositivos informáticos, sendo assim vítimas potenciais de cibercrimes. Ainda podemos destacar o crescente mercado ilegal de venda de informações, no qual empresas figuram como principais alvos de crimes contra o patrimônio, que são praticados por meio da intrusão em sistemas informáticos.

Constatamos assim que, os benefícios trazidos pelas tecnologias de informação e comunicação e que são implantados nos objetos, deixando-os com uma capacidade de autonomia, a qual é alimentada pela inteligência artificial, e capaz de prover maior comodidade, podendo, também, ser uma arma poderosa caso a sua utilização não seja adequada, moderada e segura.

2.4 – Cibercrimes

Para tratarmos do conceito de cibercrime, precisamos, primeiramente, de nos reportar ao novo espaço, não mais físico, mas virtual, denominado ciberespaço que, de acordo com (Gibson, 2003), assim é definido "*O cyberespaço, é uma representação física e multidimensional do universo abstrato da 'informação'. Um lugar para onde se vai com a mente, catapultada pela tecnologia, enquanto o corpo fica para trás*". Ainda, na mesma obra, o autor vai mais além afirmando que o ciberespaço é:

> Uma alucinação consensual vivida diariamente por bilhões de operadores autorizados, em todas as nações, por crianças aprendendo altos conceitos matemáticos[...]. Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano. Uma complexidade impensável. Linhas de luz abrangendo o não-espaço da mente; nebulosas e constelações infindáveis de dados. Como marés de luzes da cidade (Gibson, 2003).

Neste novo ambiente, surgem os cibercrimes (Machado, 2017) que são aqueles realizados pelos meios digitais, utilizando-se da Internet ou de sistemas informáticos, causando danos aos bens juridicamente tutelados, como: a vida, a honra, a liberdade individual, o património, entre outros.

Assim os delitos que eram praticados utilizando de ferramentas reais e humanas estão dando lugar àqueles que usam recursos tecnológicos. Tem, todavia, como elemento de continuidade, a obrigatória interferência do ser humano, que, se valendo desses dispositivos, cometem crimes que garantem probabilidades de lucros significativos e de menores riscos à integridade física do criminoso, pois em se tratando de ciberespaço, é mais complexo identificar e localizar o agente delituoso e este, não está fisicamente implicado.

Acrescentamos que a maioria dos cibercrimes não ocorrem no ciberespaço conhecido pela maioria das pessoas que acessam a Internet e sim um ciberespaço obscuro denominado de *Dark Net* (rede escura), que de acordo com Michael Bergman (Bergman, 2012)

> É um grupo de sites e páginas ocultas, que podem conter informações relevantes e comuns, de determinados grupos e clãs, que apenas prezam a privacidade e não querem ser importunados pelos usuários da Web, ou pode também contemplar criminosos virtuais, os mais temidos Hackers, que se beneficiam do anonimato

> desta esfera para compartilhar vírus, hoaxes entre outras atividades consideradas crimes virtuais, e até mesmo pessoas que divulgam conteúdos impróprios como pornografia infantil, locais e transações de vendas de entorpecentes, venda de órgãos, seitas satânicas, entre outras ocupações vedadas de divulgação (Bergman, 2012).

Inferimos então que existe uma "escola" em que se é possível praticar os mais variados tipos de delitos praticados em ambientes virtuais, com maior tranquilidade, tendo em vista que o acesso a esta rede de computadores obscura torna o trabalho das autoridades competentes ainda mais difícil. Ainda podemos perceber que o termo crime virtual é mal-empregado e só tem uso na linguagem popular, já que o que existe são crimes reais praticados por meio de dispositivos informáticos, seja, totalmente em âmbito virtual ou previamente neste, atraindo as vítimas para o cenário real, como por exemplo, o estupro de vulnerável, popularmente e erroneamente denominado crime de pedofilia.

2.4.1 – Cibercrimes próprios ou puros e impróprios ou impuros

Podemos definir os cibercrimes próprios ou puros como sendo aqueles nos quais o bem jurídico é o próprio sistema tecnológico, ou seja, os dados e os dispositivos que podem ou não estar conectados em rede. Assim sendo, nasceu uma nova modalidade de tutela, a que se designa por, inviolabilidade das informações informatizadas.

Por outro lado, temos os cibercrimes impróprios ou impuros, que reconhecemos como aqueles que utilizam os dispositivos informáticos apenas como uma ferramenta para praticar condutas ilícitas e violar os bens jurídicos tutelados que podem ser executados por outros meios diferentes dos tecnológicos, como por exemplo, o furto (Almeida, 2015).

Acrescentamos que, em julho de 2004, entrou em vigor a chamada Convenção de Budapeste ou Convenção sobre a Cibercriminalidade (Antonelli, 2011), que foi considerado o primeiro tratado internacional que objetivava a tipificação dos principais crimes cometidos através da Internet e de outras redes de computadores. Esta veio a estabelecer uma política criminal comum, harmonizando as leis nacionais, para melhor combater os delitos que possuem relação com redes de computadores em geral, em especial a Internet.

No Brasil, a lei nº 12.737 de novembro de 2012, conhecida como lei Carolina Dieckmann, veio acrescentar ao código penal os artigos 154-A e 154-B, tratando sobre os crimes de informática puro ou próprios, protegendo os dispositivos tecnológicos. Todavia, os crimes informáticos impuros ou impróprios, continuaram a ser tratados como delitos comuns, já que utilizam os sistemas informáticos apenas com ferramenta para tais práticas.

Partindo de tais conceitos, inferimos que junto com a era digital que vivemos, os criminosos que se utilizam de dispositivos informáticos para praticar cibercrimes necessitaram evoluir, no sentido de dominar as ferramentas para praticar estes tipos de delitos, ou a depender do caso, utilizá-la apenas como estratégias para atrair suas possíveis vítimas, como por exemplo, usar as redes sociais para cometer o crime de estelionato.

2.4.2 – Alterações e inserções que modificaram o Estatuto da Criança e do Adolescente por meio da Lei 11.829/08.

No Brasil, existem diversas legislações em vigência, dentre elas, a lei 8.069/90, denominada de Estatuto da Criança e do Adolescente (ECA), a qual tem como finalidade tipificar os direitos das crianças e dos adolescentes, como pode ser demonstrado com o texto trazido pelo artigo 1º, a saber, "*No Art. 1º, Esta Lei dispõe sobre a proteção integral à criança e ao adolescente*". Esta lei ainda vem a descrever as sanções aplicadas para quem praticar crimes contra crianças e adolescentes, além de prever, também, punições aos menores que praticarem infrações penais.

A entrada em vigor da lei 11.829/08 trouxe uma série de alterações que foram feitas no Estatuto da Criança e do Adolescente, tendo estas a finalidade de coibir e de punir a prática de delitos os quais são executados, na maioria dos casos, por meio da Internet, fins estes, dispostos do texto legal, que traz:

> Altera a Lei no 8.069, de 13 de julho de 1990 – Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, à venda e à distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na Internet (Brasil, 2008).

A lei, em comento, alterou as redações referentes aos delitos tipificados nos artigos 240 e 241 do ECA, e ainda veio a acrescentar tipos penais novos, os quais estão descritos nos artigos 241-A, 241-B, 241-C, 241-D e 241-E.

O artigo 240 e seus parágrafos primeiro e segundo, e este último com três incisos, vem a tipificar, tanto as condutas como suas respectivas sanções para o agente que dirigi, filma, produz ou fotografa, cenas de sexo explícito ou pornográfico, que tenha a participação de criança ou adolescente. O parágrafo primeiro traz a equiparação do delito, ou seja, o sujeito ativo terá as mesmas penas, quais sejam, de 4 (quatro) a 8 (oito) anos de reclusão cumulada com multa, caso venha a agenciar, facilitar, coagir ou intermediar esse envolvimento de crianças ou de adolescentes. E o parágrafo segundo aplica aumento de pena quando o crime é cometido por determinados agentes os quais possuem mais facilidade na prática delituosa, devido a uma maior proximidade com a vítima, sendo em razão da função (médico, professor etc.) que ocupa na sociedade, seja por parentesco (pai, tio, mãe etc.), ou qualquer outro meio. Vejamos a redação trazida pelo tipo penal, que dispõe (Brasil, 1990):

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento (Brasil, 1990).

O legislador ainda se preocupou em aplicar sanção para o agente que vender (inclusive por meio da Internet) ou expor à venda material pornográfico nos quais estejam envolvidas crianças ou adolescente, conforme disposto: "*Art. 241. Vender ou expor à venda fotografia,*

vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa".

É notório que os legisladores, ao acrescentar o artigo 241-A, voltaram a sua atenção para os meios virtuais de comunicação, pois os estudos que vem sendo desenvolvido no transcorrer desta pesquisa, mostram a utilização de ferramenta informáticas, as quais estão evoluindo cada vez mais rápido desde o final do século XX (FGV, 2017). Outrossim, a redação do artigo, em conjunto com os seus parágrafos e incisos, trouxe a punição para quem transmitir, disponibilizar, publicar, divulgar etc., fotos, vídeos e outros materiais que contenham cena de sexo explícito ou de pornografia com crianças e adolescente (Brasil, 1990). Destaca-se, todavia, a punição aplicada ao responsável legal da prestação de serviços, que embora tenha sido notificado oficialmente, não desabilita o acesso ao conteúdo proibido, como exemplo, temos o proprietário de um Website.

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo (Brasil, 1990).

Em continuidade, teremos o artigo 241-B, o qual punirá o agente que adquirir, possuir ou armazenar (em computadores, celulares e outros), os materiais referentes aos artigos anteriores. O parágrafo primeiro traz uma causa de diminuição de pena, qual seja, de dois terços, quando for pequena a quantidade de material encontrado. Já, o segundo parágrafo exclui tipicidade do facto, quando a posse ou o armazenamento desse conteúdo ilícito tiver a finalidade de comunicar as autoridades competentes. No último parágrafo do artigo comentado, teremos

uma solicitação de sigilo, por parte do agente que tiver o material ilícito, com objetivo de garantir êxito da investigação (Brasil, 1990). Tal artigo está assim redigido:

> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido (Brasil, 1990).

O terceiro artigo que foi acrescentado ao ECA, 241-C, vem a punir a adulteração, a montagem ou a modificação de imagens, seja por qualquer meio de representação visual que contenha crianças ou adolescente envolvidas em cenas de pornografia ou de sexo explícito. No parágrafo único, encontramos o delito em sua forma equiparada, ou seja, condutas que terão as mesmas penas (Brasil, 1990).

> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo (Brasil, 1990).

Visando a uma melhor compreensão do artigo 241-D, se faz necessário entendermos o conceito de ato libidinoso. Assim, utilizar-nos-emos dos ensinamentos trazidos pelo professor Rogério Sanches (2016), que assim se explica:

> A expressão "ato libidinoso" é bastante ampla, porosa e, se não interpretada com cautela, pode culminar em séria injustiça, como já registrada pela nossa jurisprudência quando os Tribunais subsumiam ao tipo, o simples beijo lascivo. Deve o aplicador aquilatar o caso concreto e concluir que o ato praticado foi capaz de ferir ou não a dignidade sexual da vítima com a mesma intensidade de uma conjunção carnal. Como exemplo citamos o coito *per anun*, *inter femora*, a *fellatio*, o *cunnilingus*, ou ainda a associação da *fellatio* e o *cunnilingus*, a cópula axiliar, entre os seios, vulvar etc. (Brasil, 1990).

Agora que já conhecermos o significado do termo ato libidinoso, avançaremos para as condutas tipificadas pelo estatuto no seu artigo 241-D, as quais, em seu caput, incrimina o agente que assediar, instigar, aliciar ou constranger a vítima, para que esta pratique tal ato (Brasil, 1990). E o parágrafo único, descreve as ações em suas formas equiparadas, ou seja, impõe as mesmas penas do caput (caput é um termo em latim que significa 'cabeça'. É utilizado em textos legislativos para se referir à parte principal de um artigo).

> Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Nas mesmas penas incorre quem:
> I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita (Brasil, 1990).

Finalmente, o último artigo 241-E, que fora acrescentado ao estatuto da criança e do adolescente, o qual trata de um tipo penal explicativo, tendo em vista que traz o conceito de cena de sexo explícito ou pornográfica, o qual entendemos como (Brasil, 1990):

> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos

> órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais (Brasil, 1990).

Como se percebe, a maioria dos artigos acrescentados ao ECA, por meio da lei 11.829/08, são do tipo misto alternativo, ou seja, possuem vários verbos no núcleo do tipo penal. Assim sendo, se o agente praticar mais de uma ação descrita, sendo no mesmo contexto fático, este irá responder criminalmente por crime único, levando em consideração o princípio da alternatividade.

2.4.3 – Inserção de crimes informáticos previsto no artigo 154-A do Código Penal Brasileiro feita pela lei 12.737/12

Com o surgimento da lei 12.737, de 30 de novembro de 2012, a qual ficou conhecida como lei Carolina Dieckmann, que trata dos crimes informáticos, ou seja, aqueles que possuem como alvo os dispositivos de informática, o código penal brasileiro sofreu relevante alteração, pois começou a abordar um assunto que, até então, não possuía tipificação específica (Eliezer & Gárcia, 2015).

O legislador, ao acrescentar ao código penal o artigo 154-A, resolveu colocar este dentre os delitos praticados contra a inviolabilidade dos segredos, levando em consideração que, na atualidade, os computadores armazenam as mais variadas informações, sejam de cunho profissional ou pessoal.

Antes do surgimento e da entrada em vigor da lei supracitada, as condutas criminosas praticadas com a utilização de dispositivos de informática ou contra estes, eram tratadas como delitos comuns, ou seja, com a mesma tipificação dada aos crimes praticados no mundo real, como por exemplo, furto, dano, estelionato dentre outros. Por outro lado, muitas condutas, por não existir uma tipicidade específica, deixavam de ser punidas, já que se tratava de facto atípico.

A lei 12.737, de 30 de novembro de 2012, ao entrar em vigor, acrescentou ao código penal brasileiro o artigo 154-A e seus parágrafos, o qual dispõe do seguinte título: invasão de dispositivo informático. Tal tipo penal vem a punir a conduta do agente que invadir dispositivos informáticos, que estejam ou não conectados em rede de computadores (Brasil, 1940). Vale

ressaltar que, tal conduta deve ser praticada com dolo específico de obter, adulterar ou destruir dados ou informação.

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (Brasil, 1940).

No artigo 154-A, teremos a prática do delito quando o agente invadir dispositivo informático de propriedade alheia ou instalar programas que tragam vulnerabilidade, utilizando-se dos mais variados métodos e técnicas, sem nenhum tipo de autorização do titular deste. Vale ressaltar que tal comportamento delituoso deve vir acompanhado de dolo específico, qual seja, obter vantagem ilícita.

Ao tratar de dispositivos, devemos entender que estão inseridos computadores de mesa, notebooks, laptops, smartphones dentre outros, estando estes conectados a uma rede de computadores ou não (Almeida, 2015).

O parágrafo primeiro trata do delito por equiparação, assim, terá a mesma pena o agente que realizar a produção, o oferecimento, a distribuição, a venda ou a difusão de programas específicos para praticar as condutas trazidas pelo artigo 154-A.

No segundo parágrafo, temos causa de aumento de pena quando a invasão ocorrida no dispositivo trouxer prejuízo econômico para o proprietário, ou seja, para a punição mais rígida se faz necessário o resultado material.

No parágrafo três, teremos a forma qualificada do crime, pois na conduta delituosa, houve a obtenção de conteúdos sigilosos ou secretos, os quais são protegidos por lei e podem acarretar prejuízos irreparáveis e imensuráveis. Em seguida, temos causas de aumento de pena caso esses segredos venham a ser divulgados, transmitidos ou comercializados.

Outra causa de aumento de pena vem no quinto e no último parágrafo, o qual traz proteção a algumas autoridades governamentais, que devem ter a máxima segurança de seus dados, já que fazem parte do governo brasileiro e dispõe de informação de importante relevância para o país.

A Constituição Federal Brasileira traz em seu artigo 5º, X, a proteção de direitos à inviolabilidade da intimidade, da vida privada, da honra dentre outros. Logo, as tipificações trazidas pelo artigo 154-A se enquadram dentro destas tutelas. Importante salientar, a figura do sujeito passivo, que de acordo com Márcio André Lopes Cavalcante (2012) é:

> Em regra, a vítima é o proprietário do dispositivo informático, seja ela pessoa física ou jurídica. No entanto, é possível também identificar, em algumas situações, como sujeito passivo, o indivíduo que, mesmo sem ser o dono do computador, é a pessoa que efetivamente utiliza o dispositivo para armazenar seus dados ou informação que foram acessados indevidamente. É o caso, por exemplo, de um computador utilizado por vários membros de uma casa ou no trabalho, onde cada um tem perfil e senha próprios. Outro exemplo é o da pessoa que mantém um contrato com uma empresa para armazenagem de dados de seus interesses em servidores para acesso por meio da Internet (“computação em nuvem”, mais conhecida pelo nome em inglês, qual seja, *cloud computing*) (Cavalcante, 2012).

Inferimos que a entrada em vigor do artigo 154-A foi o início de um grande e importante passo para a criação mais minuciosa de leis específicas que venham a tipificar criminalmente os mais diversos comportamentos delituosos os quais podem ser praticados por intermédio de dispositivos informáticos, em especial os conectados à Internet.

2.4.4 – Reflexões breves sobre as penas aplicadas para cibercrimes no Brasil

Após a apresentação da legislação, o delito que foi acrescentado ao código penal brasileiro, assim como as penas aplicadas para quem infringir tal norma, podemos tirar algumas conclusões sobre a posição tomada pelo legislador em criar este dispositivo.

Antes de refletirmos sobre as penalidades aplicadas aos cibercrimes próprios, é importante lembrar que a maioria dos delitos, denominados cibercrimes impróprios, praticados pela Internet são enquadrados nos tipos penais comuns, como se praticados no mundo real fossem.

A pena trazida pelo artigo 154-A, caput do código penal é de detenção de 3 (três) meses a 1 (um) ano, somado com multa. Podemos notar que tal penalidade é muito branda, em se tratando de delito que pode acarretar irreparáveis prejuízos morais e materiais. Ainda podemos acrescentar os benefícios os quais o infrator poderá se utilizar, quais sejam, transação penal[1], suspensão condicional do processo[2] e outros.

Os parágrafos que constituem o artigo 154-A trazem aumento de pena e assim como a modalidade qualificada do crime de invasão de dispositivos de informática, ainda assim as sanções permanecerão branda, podendo obter benefícios legais, de tal modo que o autor saia praticamente ileso.

[1] Art. 76. Havendo representação ou tratando-se de crime de ação penal pública incondicionada, não sendo caso de arquivamento, o Ministério Público poderá propor a aplicação imediata de pena restritiva de direitos ou multas, a ser especificada na proposta. Recuperado em 22 de novembro, 2020, from *http://www.planalto.gov.br/ccivil_03/leis/l9099.htm*.

[2] Art. 89. Nos crimes em que a pena mínima cominada for igual ou inferior a um ano, abrangidas ou não por esta Lei, o Ministério Público, ao oferecer a denúncia, poderá propor a suspensão do processo, por dois a quatro anos, desde que o acusado não esteja sendo processado ou não tenha sido condenado por outro crime, presentes os demais requisitos que autorizariam a suspensão condicional da pena (art. 77 do Código Penal). Recuperado em 22 de novembro, 2020, from *http://www.planalto.gov.br/ccivil_03/leis/l9099.htm*.

A lei 12.737, de 30 de novembro de 2012, intitulada Carolina Dieckmann, é alvo de muitas críticas pelos estudiosos do direito penal, pois por exemplo, não pune a invasão do computador que não tiver um mecanismo de segurança, ou seja, se for um usuário leigo que não se atente para instalação de antivírus, configuração de *firewall*, ou qualquer outro mecanismo, não será amparo pela lei. De tal modo, não se pune a conduta de quem invade dispositivo próprio, assim, o dono de um cibercafé pode ter acesso aos dados deixado pelos clientes nos computadores ali disponibilizado para a locação (Sanches, 2018).

Apesar de alguns artigos tratando sobre o tema, o Brasil ainda não possui uma legislação mais específica para o combate aos crimes praticados por meios da Internet. E, no atual cenário, no qual ocupamos a posição do país, dentre os cinco com maiores números de acesso, já seria exigível a criação de uma norma especial para olhar com serenidade a prática de delitos como ciberbullying, ciberstalking, sextorsion, pedofilia infantil, pornografia infantil, crimes de vingança, crime de ódio e, até mesmo, os delitos contra honra que na, sua maioria, são praticados por intermédio das redes sociais.

Percebemos que, depois de uma breve reflexão sobre as punições encontradas no ordenamento criminal brasileiro, e sabermos o quanto o mundo digital cresce com enorme rapidez, tendemos a fomentar a prática de cibercrimes, pois a sensação de impunidade irá prevalecer entre os cibercriminosos.

2.5 – Sociedade digital

Para melhor entendermos o que é sociedade digital, devemos partir do conceito de sociedade que surgiu em tempos bastante remotos, e que, no entendimento mecanicista, (Bonavides, 2012) é um "[Sociedade] *grupo derivado de um acordo de vontades, de membros que buscam, mediante o vínculo associativo, um interesse comum impossível de obter-se pelos esforços isolados dos indivíduos*".

Com a evolução tecnológica, passamos a ter o conceito de sociedade digital, que teve o seu marco inicial em meados da década de 90, quando estudiosos afirmaram que o mundo estava recorrendo a uma linguagem comum, denominada digital. E, a partir daí, a sociedade

encontrou numa nova forma de interação, por meio de ferramentas tecnológicas que encurtaram as distâncias, fazendo com que povos de diferentes culturas se comuniquem e ampliem a sua rede de relacionamento, podendo, essas relações sociais influenciarem em diversas áreas como economia, cultura, educação, dentre outras.

A sociedade digital tem uma importante participação não só na vida particular dos que nela estão conectados, como uma maior interação de forma mais ativa na política e nas decisões que influenciam o governo, tendo em vista a "voz" da população, ganha força nos canais de comunicações virtuais, trazendo à sociedade uma maior participação juntos aos seus governantes, exercendo a verdadeira democracia (SILVA, 2013).

A grande influência das tecnológica na sociedade traz mudanças significativas no comportamento das pessoas, todavia, devemos lembrar que muitas dessas pessoas serão responsáveis pelo desenvolvimento tecnológico, fazendo assim, com que seu comportamento possa interferir na criação de novas ferramentas tecnológicas, podendo se propagar e modificar o comportamento da sociedade que vive neste contexto digital, tendo como base, as suas ideias pessoais.

A criação de laços sociais trazidos pela sociedade digital fez com que surgissem novos padrões de organização, todavia é inevitável que os conflitos ocorram, assim como são comuns na sociedade tradicional, e ocorrendo tais, a tecnologia proporciona recursos para que se inicie uma guerra virtual, na qual os delitos poderão ser facilmente cometidos, como por exemplo, os que atingem o bem jurídico, honra.

Não podemos deixar de falar que o desejo de estar incluído em um mundo digital, fez com que os índices de crimes praticados contra o patrimônio começassem a crescer, em especial, o roubo e o furto de *smartphones*, já que a evolução desses dispositivos acontece de forma rápida, e vem acompanhado com o desejo de consumismo presente naquele, especialmente, que não possui condições financeiras para acompanhar uma sociedade consumista e que renova os seus artefatos de forma frequente.

2.5.1 – Conceitos de cibersegurança

Primeiramente, devemos entender o que quer dizer o termo cibersegurança, e para tal vamos recorrer ao conceito trazido pela empresa de segurança Kaspersky (2020), assim como a divisão da cibersegurança, vejamos:

> Cibersegurança é a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados contra ataques maliciosos. Também é chamada de segurança das tecnologias de informação ou segurança de informação eletrônica. O termo é aplicável a uma variedade de contextos, desde negócios até computação móvel (Kaspersky, 2020).

Dentre os diversos conceitos que estão diretamente relacionados à cibersegurança, encontramos algumas categorias as quais podemos dividir, são elas: rede de computadores, segurança de aplicativos, segurança da informação, orientação e educação do usuário final, dentre outras que auxiliarão na aplicação do conceito.

Ainda é importante ressaltar que tal segurança preza, principalmente, em garantir a integridade dos dados, em especial, aos que circulam pela rede mundial de computadores e aos que estão armazenados nos dispositivos pessoais, seja de pessoa física ou empresas.

Muitas são as ameaças trazidas pela conexão dos computadores em rede, em especial, na Internet. Pois, estamos tratando de uma rede pública, pela qual os cibercriminosos (*hackers*, *crackers*, gurus e outros) buscam as suas vítimas e para tal, utilizam das mais diversas técnicas maliciosas de ataque.

Por outro lado, temos as políticas públicas associadas à cibersegurança no Brasil, como por exemplo a Estratégia Nacional de Segurança Cibernética – E-Ciber – a qual foi aprovada em 2020, fazendo parte do primeiro módulo da ENSI (Estratégia Nacional de Segurança da Informação). Assim, estabeleceram os objetivos e ações estratégicas essenciais de pontos importantes acerca da Segurança Cibernética no País, entre eles, deixar o ambiente virtual do Brasil mais confiável, ampliando a resistência às ameaças cibernéticas.

A Estratégia Nacional de Segurança Cibernética traz, ainda, que é fundamental o investimento na cultura de segurança cibernética por meio da educação dos usuários, utilizando de forma responsável dos meios digitais, através da elaboração de cursos superiores na área de

segurança cibernética, ações de conscientização da sociedade sobre a importância do tema, além de incluir a disciplina relacionada na educação básica escolar sobre o uso de maneira segura e ética da tecnologia (Santos, 2020).

Quando tratamos de cibersegurança (Militão, 2014), muitos são os conceitos a ela relacionados, dentre eles iremos destacar os seguintes:

- Ciberespionagem a qual muitas vezes é utilizada pelo Estado para recolher informações, e assim se prevenir de futuros ataques cibernéticos;
- Ciberterrorismo que se utiliza de meios para espalhar o terror entre determinadas pessoas de uma população, valendo-se para isso do ciberespaço;
- Hacketivismo que se utiliza da busca de valhas em sistemas informatizados para então invadir computadores, assim como criar malwares os quais terão finalidades específicas, a mais comum é o furto de dados importantes.

Depreendemos, assim, que o universo conceitual os quais estão envolvidas e interligadas com a cibersegurança é de uma imensidão que tende a crescer a cada instante e, muitas vezes, em velocidades difíceis de acompanhar. Deste modo, devemos sempre manter as bases de segurança dos sistemas informáticos, visando, apenas, a implementação complementar, no caso de aparição de novas ameaças cibernéticas.

2.5.2 – Criminalidade facilitada pela era digital

Com a ascensão da era tecnológica, que trouxe muitas inovações e conforto para a sociedade de modo geral, devemos ter em mente que esta abriu uma grande porta para a prática de novas modalidades de crime, que passaram a utilizar os sistemas informáticos, junto com as ferramentas tecnológicas como uma forma de violar bens jurídicos tutelados, não esquecendo que, a informação passou a ser um bem protegido juridicamente.

Ainda que a tecnologia tenha evoluído de forma rápida, devemos levar em consideração a situação de exclusão digital (Chama, 2008). Pois, aí que mora o perigo, tendo em vista que aqueles que conseguem se incluir na era digital se depararão com um mundo completamente novo que fará que este fique vislumbrado e querendo explorar tudo, fazendo assim com que

essa viagem exploratória traga um risco altíssimo, já que sua inexperiência o tornará um alvo fácil dos criminosos que agem na rede mundial de computadores.

Junto com a popularização da Internet, nasceram muitos delinquentes que se utilizam desta para promover atividades criminosas, ou seja, a quantidade de pessoas especializadas em ambiente virtual aumentou, tendo em vista o vasto número de delitos que podem ser praticados com mais segurança, e o melhor, sem sair do conforto de suas residências. Além disso, temos uma legislação que não consegue (e talvez, nem conseguirá) acompanhar os avanços tecnológicos, deixando o sistema judiciário cada vez mais fragilizado, sem falar das punições que ainda são consideradas brandas, tendo em vista o prejuízo que pode ser causado.

A elevada adesão de pessoas que se conectam na Internet, muitas vezes sem o menor conhecimento de segurança da informação, também é um fator preocupante e relevante, quando estamos tratando de cibercrimes, haja vista, o uso de técnicas de engenharia social, na qual a vítima é induzida a fornecer informações que serão essenciais para o atacante agir. Tais informações pessoais são adquiridas facilmente, pois os utilizadores das ferramentas virtuais fornecem sem perceber o risco que correm com tal conduta (Vianna, 2000).

Percebemos ainda que, o público-alvo de determinados crimes praticados por meio de sistemas informáticos, em especial contra a dignidade sexual, são crianças e adolescentes devido a sua imaturidade e a precoce entrada no mundo digital.

Não podemos deixar de mencionar que é na adolescência que o convívio social se amplia e, devido ao grande número de horas dedicada a conexão com a Internet, estes podem ser influenciados por grupos de relacionamento virtual, a entrarem no mundo dos cibercrimes para se afirmarem na sociedade digital (Silva, 2017), como por exemplo, os que praticam o *ciberbullying*, com objetivo de mostrar que são superiores aos demais, tomando atitudes agressivas.

Inferimos que o mundo virtual é muito vasto, podendo ser utilizado em favor do crescimento cognitivo, assim como um despertar ou um aperfeiçoamento para prática dos mais variáveis tipos de delitos, seja por meios virtuais ou reais. Isso tudo se dá pela grande quantidade de informação que é disponibilizada pela Internet, e o mais grave é, que quanto mais dependentes as pessoas ficam das tecnologias, mais estão propícias a sofrer graves

consequências, seja no âmbito familiar, profissional, amoroso e/ou outros (como por exemplo reputacional).

Depreendemos ainda que a criminalidade digital, no que diz respeito ao seu combate, se faz necessária uma forte interação entre órgãos de segurança pública de vários lugares, pois estes, na maioria dos casos, são praticados bem distantes do local onde habita o criminoso.

2.5.3 – A mudança na vida dos adolescentes com a era informática

Importante iniciarmos com uma percepção de que a adolescência é tida como a fase de mudanças, perpassando por momentos de autoafirmação, de rebeldia, de descobertas da sexualidade. Porém, a conclusão mais moderna que os estudos trazem é de que se trata de momento crucial da vida. Para Drummond & Drummond Filho (Drummond, 2007),

> nessa etapa do desenvolvimento, o indivíduo passa por momentos de desequilíbrios e instabilidades extremas, sentindo-se, muitas vezes, inseguro, confuso, angustiado, injustiçado, incompreendido por pais e professores, o que pode acarretar problemas para os relacionamentos do adolescente com as pessoas mais próximas do seu convívio social. Entretanto essa crise desencadeada pela vivência da adolescência é de fundamental importância para o desenvolvimento psicológico dos indivíduos (Drummond, 2007).

O desenvolvimento cognitivo é o processo no qual é ampliada a capacidade do ser humano de processar informações, o que envolve a aquisição de recursos conceituais, habilidades de percepção, aprimoramento da linguagem e vários outros aspectos que possuem relação direta com amadurecimento do cérebro (Baldissera, 2021) – nomeadamente a capacidade de lidar com princípios éticos que ajudam no discernimento do que é bem e mal, do que justo e injunto.

Neste momento da adolescência, o ego fica engrandecido e, para potencializar isso, ferramentas tecnológicas, em especial as conectadas à Internet, facilitam e engrandecem a autoafirmação dos jovens. Ainda podemos ressaltar que o tempo livre disponível pelos adolescentes agora passaram a ser ocupados pela utilização de recursos tecnológicos (Oliveira, 2017).

Por outro lado, o acesso desenfreado à Internet trouxe uma série de modificações negativas, as quais citaremos: a dificuldade em manter relações pessoais; viver em um mundo imaginário no qual a realidade nem sempre se mantém; prejudica na alimentação, pois o uso excessivo faz esquecer de se alimentar; necessidade de mostrar uma vida que nem sempre é a realidade; dentre muitos outros problemas – criando um quadro de grande stresse mental e de risco, inclusive, de saúde mental.

O grande problema gerado pelo mundo virtual é exatamente a dependência digital, tendo em vista que os adolescentes têm maior facilidade em adquirir vícios. Assim, os jovens estão trocando as conversas pessoais pelos chats, trocam os esportes (prática desportiva) por *games* (jogos) e preferem ficar horas sem fim navegando por sites a fazer a leitura de livros.

Neste mesmo sentido e contrariando prognósticos de que a tecnologia veio somente para multiplicar informações e a interação social, muitas crianças e adolescentes nunca estiveram tão desligados do mundo real. Assim, cada vez mais, estão "hipnotizados" por seus dispositivos móveis, fazendo com que ocorra a perda de vontade de estudar, de participar de brincar tradicionais ao ar livre e até de conversar os familiares. Ressaltamos que, segundo estudiosos, muitos jovens começaram a apresentar sintomas característicos de vício (adição) em equipamentos eletrônicos, resultando assim na queda no rendimento escolar, insônia e o nervosismo sem motivos aparentes (Kiefer, 2014).

Esse desperdício de tempo navegando na Internet pode trazer problemas relacionados ao desenvolvimento cognitivo deste público adolescente, proporcionando, assim, consequências que poderão influenciar na sua vida acadêmica e profissional.

É ainda importante fazermos uma ligação entre Internet e tempo, no contexto voltado ao acesso descontrolado dos adolescentes, ou seja, estes por serem considerados, muitas vezes, nativos digitais (geração nascida com a disponibilidade da informação acessível por meio dos dispositivos conectadas à Internet), utilizam uma grande parte do tempo que possui o dia, navegando e utilizando os mais variados serviços *online*. Isso dá uma sensação de estar em outra dimensão, porém, isso reduz o poder que o cérebro tem de criar imagens próprias, ententidas coloquialmente como imaginações.

Não podemos deixar de mencionar que muitos adolescentes também se encontram dentro do conceito de exclusão digital. Todavia tal realidade vem reduzindo cada vez mais, pois

com a chegada dos *smartphones*, houve uma maior facilidade em possuir dispositivos que proporcionam acesso à Internet (Unicef, 2013).

Os adolescentes costumam utilizar a Internet, basicamente, para fazer pesquisas escolares, se comunicar com outras pessoas por meio, principalmente, de redes sociais e para entretenimento como jogos, sites relacionados com os assunto dos seus interesses e outros, por curiosidade.

Inferimos, assim, que o uso das tecnologias, em especial as conectadas à rede mundial de computadores (incluindo, além da Internet e da Web, plataformas digitais e redes sociais), podem trazer benefícios e prejuízos, a depender do modo de utilização, para aqueles que se encontram em fase de formação biopsicológica, quais sejam, o público adolescente.

2.6 – Resumo do capítulo

Atualmente, não temos dúvida de que a criação da Internet revolucionou os meios de informação e comunicação entre povos do mundo inteiro. A influência dessa rede mundial de computadores foi e é significativa, sendo inclusive, um dos suportes da sociedade da informação, em que temos pessoas que passaram a depender da tecnologia para desenvolver as suas atividades em todos os setores da vida cotidiana.

A crescente adoção das tecnologias de informação está ainda em evolução, na medida em que, atualmente, dispomos de recursos não necessitando de equipamentos físicos e de infraestrutura para desenvolvermos as tarefas mais complexas, pois temos a computação em nuvem – com ela, a disseminação das plataformas digitais. E como se não bastassem os objetos das nossas empresas, residências, hospitais e outros, agora estão diretamente ligados pela Internet, podendo ser controlados até por um simples *smartphone*.

Como toda e qualquer criação, teremos um lado menos bom e com um potencial de ameaça. O surgimento de ferramentas utilizadas com objetivo de praticar delitos no ambiente virtual, levou ao nascimento de algumas denominações como cibercrimes, cibercriminosos, ciberespaço, entre outras, facilitando a vida dos delinquentes e dificultando a das autoridades. Neste ambiente digital, é bem difícil identificar o autor do crime, ainda mais quando estes atuam

em uma rede paralela denominada *Deep Web* – criando um espaço de oportunidade e de disseminação de más práticas no contexto do digital.

Foram partilhados os conceitos de cibercrime próprios e impróprios, em que o primeiro visa atingir os sistemas informatizados propriamente ditos e o segundo são os que se utilizam da tecnologia como meios para prática delituosas comuns, como furto, estelionato, calúnia, racismo e outros.

É de suma importância, considerar a legislação específica para proteção de crianças e adolescente no Brasil, da qual se retirou e explanou todos os artigos que envolvem práticas criminosas por meio da Internet contra este público adolescente, informando das suas devidas sanções penais.

Apresentamos, também, a lei 12.737/12 que acrescentou o artigo 154-A ao código penal brasileiro, tratando sobre a proteção da inviolabilidade dos segredos, em especial das informações encontradas nos dispositivos informáticos, punindo os violadores desse direito.

Após breve análise sobre o disposto no artigo 154-A, fizemos uma reflexão relacionada às penalidades aplicadas a esta modalidade criminosa, e verificamos o quão brandas são essas, fazendo com que os criminosos saiam quase impunes das suas condutas.

Embora abordado de forma superficial, no capítulo inicial, tratamos do tema sociedade da informação, o qual foi necessário aprofundar, então perpassamos pelos conceitos de sociedade para entendermos melhor sua construção e finalidade, para daí então, mostrarmos a evolução que esta sofreu com a chegada da Internet.

Dentro de todo esse contexto, verificamos a relevância dos conceitos de cibersegurança, assim como algumas terminologias relacionadas a esta, tendo em vista que estamos navegando em um mundo novo, digital, o qual traz muita vulnerabilidade, principalmente, para aqueles que não estão acostumados ou não se adequaram a era tecnológica.

A criminalidade também evolui, no sentindo de sempre ir em busca de um terreno mais fértil para atrair e lesar as suas vítimas, e o ciberespaço é um excelente lugar para colocar em prática programas maliciosos, bem como testar as suas habilidades de persuasão e obter vantagem ilícitas.

Pensando em um público específico, os adolescentes, pois estes estão em fase de desenvolvimento físico e psicológico, e devido ao engrandecimento da autoafirmação, achando que tudo sabe e já estão preparados para enfrentar os perigos do mundo. Assim, perde (ou ocupa) horas e horas de seu dia, na frente da tela dos computadores ou *smartphones*, participando de *chats*, redes sociais, *games* e outros, estando à mercê de riscos que podem trazer consequências desastrosas, tanto físicas como psíquicas.

Por fim, podemos fazer um conexão com a tríade "cibersegurança", "era digital" e "mudança na vida dos adolescentes" com a era informática, onde temos a importância da proteção no ciberespaço já que estamos vivendo uma era digital, em que adolescentes estão imersos nesse ambiente, fazendo assim com que várias alterações, principalmente nos aspectos psicológicos, sejam benéficos ou maléficos, venham a acontecer em uma velocidade cada vez maior. Logo, se faz necessário uma blindagem preventiva, para que os malefícios de um acesso desenfreado não prejudique a vida, tanto na fase juvenil quanto adulta.

CAPÍTULO 3

Ameaças e vulnerabilidades associadas aos cibercrimes com adolescentes

3.1 – Introdução

Na era digital, cada vez mais presente na vida cotidiana, os aparelhos de televisão, de rádio, e até mesmo a velha e conhecida agenda, foi dando lugar a um equipamento, que se tornou, praticamente, indispensável nos lares atuais, o computador. Por outro lado, os *smartsphones* também se tornaram acessórios da vida das pessoas, já que estes fazem o papel de computadores portáteis e, em muitas situações, também os substituem.

Começaremos falando sobre a vulnerabilidade que perfaz o público adolescente quando, sem nenhum temor, exploram vários ambientes virtuais disponíveis na rede mundial de computadores, acreditam em que não correm perigo algum.

Em um segundo momento, mostraremos, de forma conceitual, as ameaças mais conhecidas do mundo virtual, e que vêm fazendo muitas vítimas, em especial aquelas na faixa etária que englobam as crianças e os adolescentes.

Em continuidade, falaremos quais potenciais riscos de se concretizarem as ameaças existentes no uso desenfreado da Internet, em especial, por aqueles que estão em pleno desenvolvimento psicológico e, por isso, são considerados vítimas perfeitas de cibercrimes.

Em consecutiva análise, demonstraremos o importante papel dos pais e dos responsáveis na prevenção de cibercrimes, sabendo que é essencial o diálogo à proibição ou, até mesmo, à espionagem. E a falta desse acompanhamento pode inclusive gerar consequências judiciais por abandono digital.

Seguimos, então, para a responsabilidade de professores e de educadores, entendendo que as escolas são continuidade da formação de crianças e de adolescentes, e por isso seus profissionais devem sempre estar preparados para abordar e orientar sobre os temas de relevância da atualidade, e dentre estes estão, o de cibercrimes e de cibersegurança.

Em sequência, traremos o importante papel da mídia na divulgação de cibercrimes e dicas de cibersegurança, já que possuem formas de comunicação em massa capaz de influenciar subjetivamente no comportamento da sociedade, assim como atingir os mais diversos públicos e os mais longínquos povos.

Finalmente, será trazida uma reflexão sobre os perigos atuais e iminentes a que estão sujeitos, aqueles que consideramos como público vulnerável em decorrência de vários fatores que serão mostrados no transcorrer do artigo.

3.2 – Características comportamentais dos adolescentes que favorecem a sua vulnerabilidade

A adolescência é uma fase na qual o ser humano passa por um processo de desenvolvimento, e a cada dia, com a evolução da sociedade, os adolescentes tentam se adaptar as diversidades sociais, e, assim, construir sua própria identidade, se envolvendo em relações fora do contexto familiar.

A família tem um importante papel na formação e desenvolvimento comportamental dos adolescentes, já que desde a infância o modelo de comportamento social é formado através de observações de práticas dos integrantes que compõe a família, em especial, os de convivência direta. Assim, aspectos que envolve gestão familiar com regras, supervisão, comunicação utilizadas entre familiares, controle de comportamento e até mesmo relações, em sentido amplo, são fatores que podem decidir a maior ou menor possibilidade de o adolescente se portar de forma antissocial.

O psicoticismo é uma característica da personalidade dos adolescentes marcada pela hostilidade e agressividade nas relações interpessoais (Junior, 2019), e este comportamento está diretamente relacionado com a violência vivenciada dentro da família ou na comunidade a qual faz parte. Logo, há uma tendência de o adolescente reproduzir a violência sofrida ou presenciada.

Altos níveis de psicoticismo pode levar o adolescente a possuir alto grau de frieza, agressividade, impulsividade, falta de empatia, comportamento antissociais, egocentrismo etc.

que aperfeiçoam sua busca por refúgios, e estes podem ser encontrados facilmente por meio de acesso desenfreado à Internet.

A mentira é uma característica dos adolescentes, assim, a fragilidade encontrada na relação adolescente-família vem a trazer insegurança para os jovens, fazendo com que os pais sejam os maiores alvos da mentira. Ressalta-se que a figura paterna na família, que ainda é vista como o carrasco, sendo suas atuações insuficiente, muitas vezes, no aspecto emocional e afetivo, são alvos da negativa de confiança, fazendo com que os adolescentes não lhes confidenciem as suas vidas dentro e fora dos seios familiares (Martins & Carvalho, 2010).

Os adolescentes possuem como temas centrais para suas mentiras, a sua intimidade, os seus desempenhos escolares e, por vezes, os seus vícios, deixando os responsáveis totalmente desinformados, fazendo com que isso possa trazer sérias consequências.

Por outro lado, devido a necessidade de serem aceitos nos grupos de amigos, isto é, não ser visto de maneira negativa perante estes, faz com que os adolescentes tenham mais confianças neste grupo, assim como tem em seus irmãos, reduzindo significativamente a possibilidade de mentirem.

A figura dos professores surge como aqueles que os jovens menos confiam, justamente por estes terem uma ligação de confiança com os pais, fazendo com que fiquem informados sobre todo e qualquer comportamento negativo realizado pelos adolescentes (Martins, 2011).

O autor citado no parágrafo anterior, ainda ressalta que os principais motivos que levam os adolescentes a mentirem são: a falta de coragem de assumir a verdade e serem excluídos dos grupos intrapessoais; o medo de ser castigado, especialmente pelo pai, figura da família que já tratamos anteriormente como sendo do membro mais carrasco; ainda temos o orgulho que não permitem que a verdade seja dita; e a pena de ver seus pais decepcionados com resultados não esperados.

Na adolescência a busca da autoafirmação é constante, logo, os adolescentes experimentam diversos papéis e experiências as quais são avaliadas a todo momento, com objetivo de desenvolver um padrão que seja aceito pelo meio no qual convivem.

Nesta etapa da vida, por conta das diversas transformações que ocorrem, tanto física como psicológica, os adolescentes tendem a terem comportamento como oscilação de humor,

falta de cuidados para com as suas ações, dificuldade em controlar seus impulsos, aumento no interesse sexual, conflitos familiares, sensação de onipotência, dentre outros, tornando-os passíves e alvos fáceis de algozes, em especial, no ciberespaço (Caroni, 2015).

A tomada de consciência pode levar à falsa percepção por parte dos adolescentes, que acreditam ter competência suficiente para organizar as suas vidas e ter autodisciplina e controle dos seus próprios impulsos. Essa característica faz com que estes mergulhem profundamente no mundo virtual e possam se perder nas suas afirmações/crenças errôneas.

A abertura a experiências novas é muito comum nos adolescentes, pois estes estão em fase de construção das suas identidades. Porém, em se tratando de cibersegurança, podemos citar as experiências vividas em âmbito virtual, com assuntos como sexualidade, conflitos entre pares, *ciberbullying*, *ciberstalking*, exibicionismo corporal e social, dentre outros.

A diversidade faz com que a Internet seja, para os adolescentes, um terreno fértil para realização de ações que envolvem a exposição sem nenhuma ponderação das consequências que estes podem trazer. As postagens de fotos, vídeos, comentários etc., fazem com que o ciberespaço seja palco de conflitos, os quais, muitas vezes, ultrapassam o virtual e chegam à realidade, trazendo sérias consequências, gerando processos judiciais ou até mesmo crimes contra integridade física e a vida.

Os adolescentes mergulham no mundo capitalista e de consumismo, pois tendem a acompanhar o estilo de vida dos famosos da Internet. Além disso, o risco é real em se tratando de um público que parece está perdido em um universo gigantesco de coisas atrativas como drogas, conflitos entre grupos, relacionamento com estranhos, postagem ofensivas, oferecimento de nudez e muitas outras atitudes que levam o adolescente a adoecer psicologicamente e chegar ao extremo, ceifando sua própria vida (Dias, 2019).

O neuroticismo vem como uma característica a qual os adolescentes possuem e que tornam estes, fortes candidatos a problemas como depressão, ansiedade, sentimento de culpa e outros – também aqui, com situações limites que podem levar ao suicídio.

A Internet tem uma forte influência no acionamento dos sentimentos provenientes do neuroticismo, isto é, os adolescentes que usa de forma excessiva esta ferramenta, tem maiores propensões a quadros de depressão, ansiedade e isolamento social.

Como a adolescência é uma fase de descoberta de muitos fatores de vida, a Internet pode influenciar negativamente para que os adolescentes se comportem de maneira a qual trará prejuízos para sua saúde física e mental, já que neste período estes usuários tentam preencher seu tempo e seus vazios sentimentais na frente da tela de um computador, e por vezes tomam identidades falsas para se alimentar de autoconfiança (Ulloa, 2018).

Diante desses traços de personalidade dos adolescentes, os cibercriminosos aproveitam e criam técnicas que os captam facilmente para as suas armadilhas, já que percebem nesse público uma carência de afetividade interpessoal.

A aceitação social na vida dos adolescentes vem cada vez mais sendo fator determinante de comportamento seja dentro do seio familiar ou fora. Com a sociedade digital conectada à Internet, vivemos o mundo virtual de perfeição, onde as pessoas são felizes, realizam sonhos, adquirem bens e tudo isso é publicado nas redes sociais. De outro lado, temos o adolescente que toma como base tais comportamentos e repetem, para que sejam aceites pelos seus pares.

Os adolescentes têm a chamada tendência grupal, o que se dá, pela busca da identidade de si mesmo, ou seja, eles tendem a ter comportamentos iguais, vestimentas iguais, gostos musicais iguais, expressões idiomáticas próprias, justamente para ser aceites socialmente pelo grupo aos quais querem pertencer. Além disso, há uma necessidade de se intelectualizarem, em que o adolescente tem que deixar o corpo e a mente de criança, para então ter comportamentos sociais adequados. Tal envolve uma série de conflitos mentais (Amaral, 2007).

Ainda podem ocorrer as chamadas atitudes sociais reivindicadoras, que muitos jovens possuem quando não concordam com certas restrições impostas pela sociedade. Logo, procuram grupos sociais com os quais possuem semelhante pensamento ou afinidade. Desse modo, podem passar a externalizar os seus pensamentos, o que acaba por se tornar em verdadeiras ações sociais, políticas, ideológicas, culturais, entre outras. Vale ressaltar, que a Internet traz uma maior facilidade de encontrar grupos sociais com a mesma linha de pensamento, possibilitando a interação entre os seus membros, que se encontrar em lugares fisicamente distantes, porém, virtualmente próximos.

Em se tratando de cibersegurança, essa busca por aceitação, pode trazer muitos danos, pois sempre é esperada a famosa curtida ou *like*, e quando isso não acontece, aparecem as frustações que levam esses adolescentes a quadros de ansiedade e depressão, chegando muito

vezes a praticar o suicídio, se sentindo desprezados e não aceites naquele meio ao qual pretendem pertencer.

A empatia na adolescência tem uma forte relação com a forma na qual foi conduzida pelos responsáveis, fazendo com que floresça um sentimento de compaixão e compreensão para com os diferentes grupos sociais, praticando ações que mostram igualdade e valorização, ainda que diferentes ou mesmo totalmente distintos, sejam os pensamentos entres esses.

Este sentimento de compadecimento com o sofrimento alheio, pode trazer vulnerabilidade, já que cibercriminosos podem valer-se desta característica para se aproximar do adolescente, fazendo-se passar por membros de grupos aos quais as suas causas, sofrimentos e angústias são partilhados e defendidos.

Ainda na infância demonstramos o interesse de interagir com outras pessoas. Todavia, é na fase da adolescência que se aflora a necessidade dessa interação, e para isso o adolescente se entrega para terceiros. Tal comportamento é importante nesta fase da vida, fazendo com que haja uma preparação para etapa posterior; a adulta (Serafini, 2008).

A extroversão é uma característica marcante na vida dos adolescentes. Estes se sentem bem em interagir com outros, mostrando-se falante (faladores), sociáveis, entusiasmados e disponíveis. Para que cada individuo seja aceite por aqueles grupos sociais ou até mesmo por seus pares, tem de investir e partilhar características comuns.

Essa interação social tem o seu lado negativo, pois há risco de os adolescentes serem influenciados por amigos e pelos seus próprios pares. Entre os riscos podemos citar o consumo de álcool, drogas e até a prática de crimes. E, na atualidade, as tecnologias também se tornaram ferramentas aliadas para expansão, tanto das redes de comunicação quanto para as influências negativas que podem atingir os adolescentes.

A atração interpessoal, seja com amigos ou relações românticas, tem uma significância relevante no mundo social dos adolescentes. Assim, um tempo considerável do período da adolescência é voltado para pensamentos relacionados a parceiros românticos, onde estas relações surgem após os primeiros contatos com sexo oposto.

As redes sociais de interação interpessoal, possui uma importante carga na trajetória de desenvolvimento nesta fase tão importante da vida do ser humano, e a ocorrência de bons

relacionamentos entre diferentes pessoas da sociedade traz indicadores que mostram uma maior probabilidade no sucesso acadêmico, profissional, no bem-estar, conseguindo, com isso, reduzir os indicadores de problemas como depressão, ansiedade, distúrbios alimentares, dentre outras complicações físicas e psicológicas.

Importante destacar que a dificuldade dos adolescentes se relacionarem com outras pessoas, pode não ser simplesmente um processo normal para seu próprio desenvolvimento, mas, sim, problemas patológicos que devem ser tratados para que não gerem complicações maiores (Carvalho, 2013).

3.3 – Vulnerabilidade dos adolescentes

É de suma importância ressaltar que os sujeitos passivos da vulnerabilidade tratada neste capítulo têm idades que foram pré-definidas no artigo 2° do ECA (Estatuto da Criança e do Adolescente), que traz "*Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade*". Ressaltando ainda que, o artigo 3° do mesmo estatuto traz os direitos fundamentais que amparam esse público, assim descrevendo (Brasil, 1990),

> Art. 3º A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade (Brasil, 1990).

O fluxo de informação proporcionado pela Internet é imensurável, e tendo em vista essa facilidade é que os algozes agem nesse ambiente virtual, trazendo riscos, em especial, para o público adolescente, pois estes tendem a explorar o *cyber* ambiente de maneira destemida e sem nenhuma forma de cuidado, o que faz com que, muitas vezes, eles contribuam para a sua própria vitimização.

Os criminosos que agem no mundo virtual e que comentem delitos contra os adolescentes se prevalecem de alguns fatores que fazem parte da personalidade desse público, quais sejam: a autoconfiança de que nada de ruim acontecerá; o prazer de desafiar os pais; a

sensação de terem *expertise* (destreza) suficiente para navegar na Internet; busca por aventuras e por experiências novas; com exposição da vida pessoal; dentre outras iniciativas e riscos (Silva, 2009).

Este público se torna mais vulnerável, na medida em que os seus pais ou responsáveis legais, perdem o controle e deixam de monitorar o acesso à Internet dos seus filhos, que, em razão da falta de maturidade e da imensidão de conteúdo trazido pelo mundo virtual, acabam atraídos pelos criminosos que tiram partido deste cenário para a prática de delitos.

Devido à gama de informações fornecidas pela própria vítima, os abusadores criam a melhor estratégia para os atrair, seja criando perfis de pessoas da mesma faixa etária, ou verificando as preferências da sua presa, para então realizar uma aproximação.

Quando estamos tratando, exclusivamente, do público adolescente que está em pleno desenvolvimento da sexualidade, temos que estes se tornam ainda mais vulneráveis, devido a esta fase das suas vidas, ou seja, a puberdade. Além disso, destacamos que, por falta de uma melhor orientação, os de classes mais baixas são os mais atingidos (Bretan, 2012).

Constatamos assim que, os fatores de vulnerabilidade que existem, em especial, nos adolescentes, se dão por fatores biológicos, sociais e comportamentais. Porém, a falta de orientação, tanto por parte dos pais como do poder público, tende a fortalecer a facilidade de ataque a estas vítimas, em se tratando de um ambiente virtual fértil para a prática de delitos.

VULNERABILIDADES	SIGNIFICADO
Relativo à idade	O acesso às ferramentas tecnológicas com idades cada vez mais baixas.
Relativo à falta de preparação	Não maioria dos casos, crianças e adolescentes ingressam no mundo virtual sem antes ter uma orientação.
Relativo à falta de monitoramento	Os pais ou responsáveis legais, muitas vezes, não se preocupam em monitorar os acessos dos filhos.
Relativo à falta de políticas de segurança específicas	O governo não se preocupa em fazer campanhas de prevenções para os cibercrimes, e muito menos, alertas para o acesso irrestrito de crianças e de adolescente, mostrando os riscos reais.

Relativo ao vício digital	Nos dias atuais, crianças e adolescentes trocaram as brincadeiras tradicionais pelos equipamentos eletrônicos, em especial *smartphones* e computadores.

Tabela 1 – Vulnerabilidades e seus significados

3.4 – Ameaças cibernéticas associadas aos adolescentes

As tecnologias vêm despertando o interesse das pessoas há alguns anos, todavia não podemos negar que a maior afinidade e a facilidade em lidar com essas inovações vêm das crianças e dos adolescentes.

A facilidade de desenvolver as atividades diárias, seja no âmbito educacional, profissional ou ainda para o momento de entretenimento, utilizando as ferramentas tecnológicas disponíveis na Internet, vem crescendo a cada dia, apesar de ainda ter certa rejeição do público com maiores idades.

Neste cenário, em que os pais, não raras vezes, perderam o que há de mais importante na sua relação com os filhos, ou seja, o diálogo, o computador vem se tornando o melhor e mais fiel amigo das crianças e dos jovens, fazendo com que estes exponham todos os seus sentimentos aos amigos virtuais (Eisenstein, 2006).

Dentre os diversos delitos que podem ser praticados contra os sujeitos passivos em destaque, temos aqueles ditos mais gravosos, pois lesam o bem jurídico denominado dignidade sexual. Assim, denominamos, popurlamente, os crimes desta natureza como pedofilia infanto-juvenil, já que as vítimas desse ato criminoso podem ser tanto crianças como adolescentes.

É importante conhecermos o conceito dado pela Organização Mundial de Saúde para o termo pedofilia, que segundo esta é a "*Preferência sexual por crianças, quer se trate de meninos, meninas ou de crianças de um ou do outro sexo, geralmente pré-púberes ou no início da puberdade*" (OMS, 1993). Assim, podemos dizer que se trata de um desvio de conduta sexual (parafilia), ou seja, o criminoso possui uma perversão sexual, caracterizada por fantasias, anseios ou atividades incomuns que trazem sofrimento clinicamente significativo ou propiciam comportamentos sociais e ocupacionais inadequados, tendo como objeto de desejo, a criança.

Não se pode negar que a facilidade encontrada por esses pedófilos, em conseguir se aproximar das vítimas mais vulneráveis, teve um crescimento significativo após a explosão das tecnologias que estão diretamente ligadas à Internet, justificando assim, a criação de novos tipos penais, que foram acrescidos no Estatuto da Criança e do Adolescente, os quais estão voltados aos delitos praticados na rede mundial de computadores.

No Brasil, discute-se a necessidade de uma legislação ainda mais completa sobre os crimes praticados por meios da Internet, todavia existem doutrinas que divergem deste pensamento, pois acreditam em que haverá um excesso de normas, sendo tais imposições desnecessárias (Silvia, 2016).

Por outro lado, as ameaças crescem a cada dia, tendo em vista uma combinação perfeita para os criminosos, a qual se dá com facilidade que os meios virtuais proporcionam, juntamente com a dificuldade de localização dos criminosos, a falta de uma legislação mais específica e o tratamento brando que o normal quadro penal traz, ao fazer o enquadramento em legislação penal.

De acordo com a Organização dos Estados Americanos (OEA), por meio de sua agência especializada em crianças e adolescentes, o Instituto Interamericano da Criança (IIN) (Mendoza 2018), foi divulgada uma publicação sobre as principais ameaças que podem atingir crianças e adolescentes, das quais podemos citar: abuso sexual de crianças e de adolescentes na Internet; *cyberbullying*; exposição a conteúdos inapropriados; *grooming* (estratégia para ganhar confiança de criança e adolescente, usada para fins libidinosos); *happy slapping* (uma forma de cyber-violência, em que é filmado e depois postado na Internet, o ataque humilhante); *sexting* (forma de pressionar crianças e adolescentes a enviar fotos de teor sexual); *sextortion* (extorquir uma pessoa, com ameaças de enviar as suas fotos íntimas), e outras alternativas que emergem da prática continuada do uso e exploração do digital.

Inferimos, então, que as ameaças trazidas pelo uso de tecnologias ligadas à Internet podem ter as mais diversas variações, que pode culminar com delitos menos graves como injúria, calúnia e difamação, até aos mais gravosos, que são os praticados contra a vida e a dignidade sexual das crianças e dos adolescentes.

3.5 – Os aspectos de convivência entre os adolescentes, seus responsáveis e a sociedade contemporânea

Os laços afetivos familiares são considerados fatores de suma importância para o desenvolvimento social do indivíduo, isto é, a base do aprendizado que se externalizam nas interações sociais está, justamente, nos ensinamentos os quais são repassados no convívio no ambiente interno. Assim, as crianças aprendem, dentro de casa e com os seus parentes, o modo de falar, de se relacionarem, reagirem às diversas situações, interpretar o que ouvem etc. (Mota, 2019).

Importante ressaltar, o conceito de família na atualidade. Para isso, partiremos, primeiramente, do que descreve a Constituição Federal do Brasil, a qual traz em seu artigo 226, § 4º a seguinte afirmação "*Entende-se, também, como entidade familiar a comunidade formada por qualquer dos pais e seus descendentes*". Todavia, sabemos que muitos adolescentes foram criados por avôs, tios, pais adotivos, padrastos e madrastas. E isso, influência diretamente a forma de compreender e aceitar o conceito de família da era moderna.

A adolescência é uma fase marcada por constantes desequilíbrios e instabilidades, por isso, dizemos que esta etapa da vida corresponde a um fenômeno biopsicossocial, o qual sofre mutações constantes, e estas se dão por intermédio de influência da sociedade (Pratta, 2007). Embora esses fatores possam soar de forma negativa, eles são essenciais e necessários para o desenvolvimento psicológico dos indivíduos, tornando-as, assim, uma crise normativa.

As transformações que surgem na adolescência não são somente dos filhos, mas, de todo aquele seio familiar, fazendo com que os responsáveis também passem a aparentar para a sociedade que voltaram a adolescência. Logo, os pais começam a vivenciar sensações como angústias, as quais, se assemelham com as vividas nas suas adolescências.

A relação entre os pais e os adolescentes podem trazer conflitos, principalmente, pelas preocupações, em especial, com a iniciação precoce da vida sexual, tendo em vista os riscos de doenças como o HIV (Vírus da Imunodeficiência Humana) ou até mesmo gravidez indesejada, bem como a ameaça do ingresso no mundo das drogas. E, estes fatores, pode parecer fácil de ter o controle na cabeça dos adolescentes, os quais acreditam poder lidar com isso de forma

tranquila, porém, como já vimos anteriormente, é uma falsa ilusão de autocontrole e autodeterminação.

A figura dos avôs pode aparecer na criação dos adolescentes e isso implica em vários fatores como: forma de ajudar os netos a conhecerem melhor os pais; redutores da ansiedade infantil, preparando-os para uma melhor fase de adolescência; participação em vários aspectos da vida, como social, cognitivo, emocional e outros.

A relação entre os avôs e os adolescentes traz um conjunto de características, dentre as quais uma forma de corrigir ou de proporcionar para estes, aquilo que não puderam fazer com seus próprios filhos, e até mesmo uma forma de se defender da aflição trazida pela idade avançada e a morte inevitável (Dias, 2010).

Se por um lado, há inúmeras amostras de afinidade e afetividade, por outro, podemos inferir que a falta regras mais rígidas e até mesmo pelo não acompanhamento tecnológico da nova era, os adolescentes criados com avós tendem a ter mais liberdade e, até mesmo, facilidade em mentir e enganar os seus avós, colacando-se em risco iminente quando se veem livres para acessar a tudo que é possível dentro da rede mundial de computadores.

Vale ressaltar que, com o rápido amadurecimento, o qual o mundo dos adolescentes vem se apresentando, a tendência é de, cada vez mais, termos avós com pouca idade e que continuam ativos, semelhantes aos pais, isto é, acompanham o desenvolvimento cultural, social, tecnológico e outros, acompanhando a evolução da nova geração.

Os conflitos que surgem entre casais, os quais cominam em divórcios, interferem diretamente na vida do adolescente, pois estes passaram por turbulência vividas pelos seus pais antes da separação, podendo ser o gatilho para diversos problemas psicossociais.

Por outro lado, o recasamento pode trazer um equilíbrio e uma significante melhoria no comportamento dos adolescentes, quando percebem que os seus pais estão felizes e tranquilos com os seus novos pares. Isso dar a estes uma impressão de pertencer novamente a uma família completa. E este novo sentimento de tranquilidade, traz benefícios até quando os adolescentes viram adultos e saem das suas casas, pois terão a certeza de que os seus pais estarão bem acompanhados e poderão seguir o curso da vida tranquilamente (Sousa, 2014).

Os pais que decidem recasar podem virar grande exemplos para seus filhos, na medida em que esta nova família demonstra qualidade na relação existente. Isto faz com que os adolescentes tirem proveitos positivos e negativos, no que diz respeito a relacionamentos amorosos, todavia, isso não significa dizer que este terá maior ou menor bem-estar.

Como a adolescência é marcada por rebeldias, é muito importante, que os pais recasados, sejam em nova união heteroafetiva ou homoafetiva, devem rever e negociar as regras que eram aplicadas aos filhos quando crianças, e quem sabe até extinguir algumas, tendo que levar em consideração a fase de adolescência, pois este, como já falado anteriormente é um período de grandes modificações físicas e psicológicas.

Com a evolução da sociedade, hoje temos uma mutação do modelo autoritário de criação para um modelo mais democrático, principalmente em se tratando de adolescente, os quais possuem como característica o questionamento de toda e qualquer forma de restrição. Assim, para muitos autores, esse papel de educar o filho deve permanecer com o pai ou mãe, deixando um pouco de fora a figura do padrasto ou madrasta, os quais podem ajudar, porém, de forma a se tornar amigo (a) dos enteados (as), já que impor limites ou tentar disciplinar de forma autoritária irá gerar conflitos (Junqueira, 2016).

A sociedade contemporânea vem cada vez mais reduzindo a diferença entre adultos e adolescentes, já que a adolescência tende a se postergar, fazendo com que os pais assumam o papel de amigo do filho, ao invés daquela figura autoritária. Ainda podemos contemplar que os adultos tendem a experimentar as sensações de juventude, sendo obrigados a deixar o autoritarismo de lado e entrando em uma relação de amizade e democracia.

A ideologia igualitária faz os pais se apresentarem como amigos dos filhos, e isso é muito importante, até mesmo para o ganho de confiança, o que faz com que em situações de conflito, de risco ou de vitimização de um delito, seja partilhado com o responsável.

O consumismo que antes era praticamente característica dos adultos, hoje, atinge os adolescentes de tal modo que tendem a se igualar neste aspecto. Assim, a cultura da posse de bens materiais ser razão da felicidade, passou a ser comum na adolescência. Porém, vale ressaltar que, adultos e adolescentes possuem diferentes gostos de consumo, os quais irão se alterar a depender dos grupos sociais. E mesmo que haja esse igualitarismo em alguns aspectos, por óbvio, a diferença entre eles permanecem (Salles, 2005).

Inferimos que com essa tendência da sociedade contemporânea de promover a igualdade, em alguns aspectos, entre adultos e adolescentes, em especial, no acompanhamento da evolução tecnológica, no que diz respeito, principalmente, ao acesso à Internet, trazendo maior facilidade em entender e monitorar as atividades desses vulneráveis.

3.6 – Os riscos de concretização das ameaças em face à vulnerabilidade dos adolescentes

A vulnerabilidade reporta à ideia de sensibilidade ou de fraqueza relacionada com determinada área, fazendo com que aumente a possibilidade de ser afetado de alguma forma. E, em se tratando de mundo digital, este fator negativo pode interferir das mais variadas maneiras, na saúde física e, principalmente, mental das crianças e dos adolescentes (Fonseca, 2013).

Com advento das redes sociais, os riscos aumentaram significativamente, tendo em vista que agora há uma interação "real", crescendo assim também, as ameaças virtuais. Tal, deixa a vulnerabilidade do público adolescente ainda mais evidente, pois estão em fase de desenvolvimento psicológico, o que, muitas vezes, contribui para a ação dos algozes.

Podemos fazer uma reflexão, analisando o seguinte posicionamento (Pereira, 2015),

> Ao permitir a entrada de menores de idade em sites cujo objetivo é a interação social através da publicação de atividades rotineiras e exposição de fotos, acontece a superexposição da criança ou adolescente que inconscientemente atrai diversos outros perigos para si, mostrando-se vulnerável a atuações de marketing, de criminosos ou até mesmo da espionagem da sociedade (Pereira, 2015).

Os posts publicados nas redes sociais, embora pareçam algo normal e inofensivo, podem ser um forte fator de risco para os menores de idade, já que, muitas vezes, os pais, de maneira inconsciente, colocam fotos de nudez ou que identifica a sua morada, criando assim riscos, seja com maior ou menor possibilidade de ocorrência.

Devido ao grande bombardeio de informações e conceitos que são impostos pela sociedade, podemos verificar que uma simples postagem de um adolescente, por exemplo, pode

gerar uma série de críticas, transformando-se assim no conhecido e venenoso *ciberbullying*, o qual, na maioria das vezes, atinge o psicológico de forma avassaladora (Feuser, 2017).

Na perversão sexual voltada para adolescentes, podemos citar, também, como um risco iminente de ocorrer, caso fotos de nudez ou sensuais caiam nas mãos de delinquentes. Esses têm a seu favor a possibilidade de propagação de tais imagens, na denominada *Deep Web*, ou seja, uma rede obscura na qual ocorrem os mais variados delitos na Internet.

Outro problema muito presente no acesso desse público sem *expertise* é que esta inexperiência é aproveitada pelos criminosos, agindo de forma a convencer, em especial, as crianças ou pré-adolescentes a fornecerem dados relacionados com cartões de créditos dos seus pais. Para isso, criam personagens que irão interagir com essas crianças, com objetivo de obter tais informações.

O ciberespaço é considerado ambivalente, ou seja, potencialidade e risco são bem definidos. Assim, a preservação dos direitos fica iminentemente comprometida. Este acesso fica ainda mais perigoso, quando as tecnologias ligadas à Internet tornam-se rotina na vida de crianças e de adolescentes, fazendo desta, muitas vezes, uma fuga dos problemas do mundo real. Todavia, estes acabam por ingressar em um perigoso mundo virtual, em que as situações desastrosas podem tornar a vida desses vulneráveis ainda mais devastada (Souza, 2016).

Inferimos então que, por se encontrarem em processo de desenvolvimento físico e psíquico, crianças e adolescente não conseguem ter a percepção dos riscos em potencial, os quais estão expostos, sendo estes os mais variáveis, como por exemplo, *ciberbullying*, crimes contra honra, aliciamento para fins sexuais, pedofilia e muitos outros.

3.7 – Papel dos pais e responsáveis na prevenção de cibercrimes

De acordo com os textos normativos constitucionais, a família tem um nobre e árduo dever de cuidados para com os filhos, garantindo, com a ajuda do Estado e da sociedade, a proteção dos direitos a eles inerentes, vejamos como dispõe o artigo 227 da Constituição Federal Brasileira (Brasil, 1988).

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão (Brasil, 1988).

Independentemente de leis, os pais e os responsáveis sempre tiveram um papel fundamental no desenvolvimento cognitivo e emocional de seus filhos, e, por estarmos em uma sociedade de explosão tecnológica, estes devem procurar evoluir e se atualizar para melhor orientar os seus filhos com relação aos perigos existentes no mundo virtual.

A família pode ser considerada a primeira instituição formadora da sociedade, pois esta serve de espaço de aprendizagem, embora informalmente, se colocando na posição inicial para todo um processo de desenvolvimento social. Deste modo, a família acaba por transmitir a experiência e os conhecimentos relacionados a vida social, de acordo com a prática do dia-a-dia, isto é, a vivência (Yoba, 2018).

O papel educativo da família é reconhecido por Silva (2017) da seguinte maneira "*mesmo sem projecto educativo, e de forma espontânea, a família realiza a educação dos seus membros para os tornar cidadãos úteis à sociedade"*. Assim, esse pensamento a espontaneidade do processo de transmissão de conhecimentos no seio familiar, sem se preocupar com qualquer tipo de regras rígidas ou metodológicas é um dos suportes do adolescente (e seu porto de abrigo).

Muitos psicólogos aconselham que deve haver um acompanhamento dos jovens quanto à utilização da Internet, e que o melhor caminho não é a proibição e sim o diálogo franco, procurando criar cada vez mais um elo firme de confiança na relação. Do mesmo modo, especialistas, não aconselham e dizem que não é eficiente a instalação de programas espiões para monitor o que os filhos fazem na Internet, pois isso acaba por prejudicar ou até findar a confiança dos jovens (Craide, 2017).

Assim como se orienta os adolescentes para os perigos encontrados no mundo real, mostrando casos concretos para servirem de exemplos, do mesmo modo a orientação deve ser exposta com relação aos males trazidos pelo ambiente virtual, no qual, os jovens estão cada vez mais envolvidos e de forma mais profunda.

Devemos levar em consideração que os jovens não possuem desenvolvimento cognitivo avançado, bem como experiência para enxergar as vantagens e as desvantagens de um acesso desregrado na Internet. Logo, o acompanhamento dos responsáveis é de suma importância e garantirá o uso salutar da tecnologia (Tibúrcio, 2019).

A doutrina brasileira já deu início ao reconhecimento de novo conceito para responsabilizar aqueles que têm o dever de cuidados para com os menores, no que diz respeito ao uso de recursos tecnológicos ligados à Internet, este foi denominado "abandono digital" e pode trazer consequências jurídicas em caso de omissão desses cuidados (Klunck & Azambuja, 2020).

Depreende-se que, assim como os pais e responsáveis legais sabem, ou ao menos deveriam saber, por onde os filhos andam no mundo real, devem ter o mesmo conhecimento quando se trata de ciberespaço, ou seja, ter a certeza dos sites acessados, jogos que participam, pessoas as quais mantém contato, grupos que participam, dentre outras atividades disponibilizadas pela Internet. Assim, o risco de os filhos serem vítimas e, até mesmo autores de infrações penais, reduzem de forma significante.

3.8 – Professores e educadores trazendo a temática (cibercrimes e cibersegurança) para dentro das salas de aula

Não podemos negar que a sala de aula é um espaço inesgotável de aprendizagem, desde a infância até a fase adulta. O ser humano é um eterno aprendiz e, na figura dos professores, muitas vezes, surgem as inspirações ou até uma imagem de um futuro promissor.

O uso de ferramentas tecnológicas está cada vez mais presente, atualmente, nas escolas, fazendo com que os professores e os educadores necessitem de estar em constante aperfeiçoamento para fazer o acompanhamento dos alunos e, acima de tudo, orientar da melhor maneira possível, para que estes diminuam a possibilidade de serem vítimas de cibercrimes (Macedo, 2018).

Levar para dentro da sala de aulas, temas como *ciberbullying*, *sexting*, crimes de ódios, automutilação e outros, praticados por intermédio da Internet, é de um grau de importância, que

em nosso momento contemporâneo, podemos equiparar às demais disciplinas ensinadas, tendo em vista, a preocupação, inclusive, com a saúde mental dos alunos, em especial os adolescente.

É muito importante que os professores abordem e discutam com os alunos factos ocorridos no Brasil e no mundo, onde crianças, adolescentes e, até mesmo adultos, foram vitimizadas pelos cibercrimes. Logo, mostrar através de exemplos verídicos, como os cibercriminosos agem e quais as ferramentas e meios eles utilizam, irá reduzir a possibilidade dos ouvintes serem, também, vítimas. Além do que prenderá a atenção dos alunos, os quais podem servirem como facilitadores para outros.

Apesar de alguns professores conhecerem o conceito de cibercrimes, acreditamos que a maioria não é conhecedora de técnicas para se proteger contra estes. Além disso, pouquíssimos são aqueles interessados em se aprofundar no assunto, para então poderem repassar aos alunos, reduzindo assim a vulnerabilidade destes.

A escola é o lugar no qual se inicia o ciclo da vida em sociedade, em que, apesar de sermos e termos comportamentos e opiniões diferente, aprendemos a respeitar a do outro. Assim, a responsabilidade da escola não estar restringida somente por manter a integridade física dos seus alunos, mais principalmente, a sua integridade moral (Borelli, 2016) e porque não dizer a psicológica, também. Isso pode ser ratificado com o texto trazido pelo artigo 2º da lei 9.394/96 (Lei de diretrizes e bases da educação nacional), que assim dispõe: "§ 2º *A educação escolar deverá vincular-se ao mundo do trabalho e à prática social*" (Brasil, 1996).

De acordo com Duarte (2013), é importante o papel da educação escolar no que diz respeito ao desenvolvimento da personalidade dos adolescentes. Assim, é o compartilhamento do desejo de sempre aprender, isto é, mergulhar no mundo do conhecimento que ainda deve propmover a curiosidade e a experimentação. Assim, deve ser realizada uma mediação entre a vida cotidiana e a não cotidianas pautada nos objetivos do ser humano. (DUARTE, 2013).

A lei 8.069/90 (Estatuto da Criança e do Adolescente) traz uma ratificação do que dispõe a lei supracitada, pois o seu artigo 53, menciona: "*A criança e o adolescente têm direito à educação, visando ao pleno desenvolvimento de sua pessoa, preparo para o exercício da cidadania e qualificação para o trabalho*".

No Brasil, em 2015, entrou em vigor a lei 13.185/15 a qual "*Institui o Programa de Combate à Intimidação Sistemática (Bullying)*". Em seu artigo 1º, § 1º é introduzido o conceito

de intimidação sistemática (*bullying*), na qual sabemos que ocorrem na grande maioria das vezes, por meio da Internet, vejamos:

> Art. 1º Fica instituído o Programa de Combate à Intimidação Sistemática (Bullying) em todo o território nacional. § 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática (bullying) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas (Brasil, 2015).

Em continuidade ao conteúdo da mencionada lei, verificamos, claramente, a responsabilidade a qual foi atribuída às escolas. Recorremos ao artigo 4º, inciso II, para suporte das nossas posições, este traz: "Art. 4º – *Constituem objetivos do Programa referido no caput do art. 1º: II – capacitar docentes e equipes pedagógicas para a implementação das ações de discussão, prevenção, orientação e solução do problema*" (Brasil, 2015).

O Ministério Público Federal apresentou um movimento que tem por objetivo a conscientização das pessoas em relação ao uso da Internet, mostrando que muitas das condutas adotadas pelos usuários são consideradas criminosas e podem trazer consequências desastrosas como a punição de restrição da liberdade (Gandra, 2020).

Entende-se, assim, que várias são as formas desse conhecimento sobre cibercrimes chegarem até a equipe de profissionais, os quais atuam nas escolas, e que pode variar desde as pesquisas realizadas na própria Internet até palestras ofertadas por órgãos públicos que dizem respeito ao tema mencionado. Por outro lado, os responsáveis pela educação devem motivar os seus professores, assim como contar com a boa vontade de cada um, para que juntos possam se fortalecer com conhecimento específico e consequentemente partilhado com os alunos, para os tornarem mais imunes aos ciberataques.

3.9 – A importância da mídia na divulgação de cibercrimes e dicas de cibersegurança

A comunicação em massa tem importante papel na sociedade contemporânea, a qual com auxílio de tecnologias, vem se aprimorando a cada dia e assim, fazendo com que as

informações ultrapassem fronteira em velocidade cada vez maior. Assim, a mídia faz parte da história humana, no sentido de desenvolvimento entre os membros da própria sociedade, fazendo parte do cotidiano e tendo influência, inclusive, nas alterações de comportamentos.

Com a chegada da Internet, devemos destacar que a evolução da mídia deu um salto extremamente considerável no sentido de facilitar a publicidade e os meios de comunicação entres todas as sociedades do mundo inteiro. Se, por um lado, essa explosão tecnológica no mundo da mídia trouxe maravilhosos benefícios, por outro, a forte influência, negativa ou positiva, deve ser levada em consideração e tomada em devida conta.

A Internet apareceu na mídia como uma inovadora e forte responsável pela influência da subjetividade, pois além da rápida disseminação de informações, ela encurtou os mais longínquos povos, ou seja, atravessar o mundo agora é possível com alguns *clicks*. Então fica clarividente que a divulgação de cibercrimes e de cibersegurança, por meio desse novo conceito de mídia, e de grande e notória eficiência (Moreira, 2010).

Podemos considerar a mídia da Internet mais eficiente no processo de produção de subjetividade, e devido ao volumoso público e ao tempo de acesso destes no mundo virtual, inferimos uma eficácia significativa, na divulgação dos modos de reconhecimento e de prevenção nas ações praticadas pelos cibercriminosos, e estas informações atingirão todos os públicos, desde os pais, até aos gestores do Estado.

No Brasil, temos três poderes: o executivo, o legislativo e o judiciário, e para alguns autores a imprensa pode ser considerada como o quarto poder, devido ao potencial que possui para influenciar nas decisões da sociedade. Vejamos o testemunho de Darci Miranda (1995),

> A verdadeira missão da imprensa, mais do que informar e divulgar factos, é a de difundir conhecimentos, disseminar a cultura, iluminar as consciências, canalizar as aspirações e os anseios populares, enfim, orientar a opinião pública no sentido do bem e da verdade (Miranda, 1995).

Hoje, a mídia é capaz de implantar pensamentos e opiniões nas mentes das pessoas, de tal forma, que podem impactar em decisões as quais traçam o destino de uma pessoa, como por exemplo, os casos de grande repercussão, julgados pela justiça criminal (Fernandes, 2016).

Com a chegada das redes sociais, a mídia aderiu essa poderosa ferramenta para comunicação e propagação de conteúdos informativos. Este mesmo recurso é utilizado para

promover manifestações e mobilizações de grande escala, e, por esse motivo, podem ser usadas para estimular e conquistar mudanças na sociedade, tal como sendo de participação relevante no combate aos cibercrimes contra adolescentes (Barros, 2012).

Não se pode negar que, o público adolescente, na atualidade, gastar várias horas de seu dia navegando nas redes sociais, ou seja, estas seriam uma boa oportunidade para disponibilizar conteúdos educativos relacionados aos cibercrimes, aos cibercriminosos e à cibersegurança. Assim, afastando inclusive a incidência de crimes praticados por intermédio destas próprias ferramentas de comunicação social, as quais são palco de *ciberbullying*, de pornografia infantil, de crimes de ódio, entre outros.

Entendemos, então, que todas essas demonstrações de força e de poder de retórica encontrado nas mídias, tanto as impressas quanto as digitais servem para nos mostrar o quão importante seria a divulgação em massa de temas relacionados aos cibercrimes. Ainda mais valioso, e de grande relevância, seria propagar os mais diversificados meios de prevenção contra estes delitos.

3.10 – Reflexão dos cuidados do acesso à Internet feito por adolescentes

Atualmente, sabemos que a Internet tem como realidade um vasto terreno nocivo, e que devido ao grande número de programas utilizados como mecanismo para proteção dos usuários, os criminosos especializados nos ataques virtuais conseguem camuflar as suas ações, passando por cima das barreiras de proteção, já que a obscuridade e a extensão espacial proporcionada pelo acesso tornam a segurança difícil ou até mesmo impossível de ser combatida de forma absoluta.

Partindo da ideia de que as crianças e os adolescentes acessam a rede mundial de computadores sem nenhum temor, o melhor caminho seria, de facto, a orientação no uso desenfreado, assim como mostrar os riscos e ensinar a identificá-los, fazendo com que sejam criados por esses usuários, os seus próprios mecanismos de defesa. Tendo em vista que, na atualidade, a Internet e os seus perigos são incontornáveis, a prevenção se mostra mais eficiente do que a proibição (Monteiro, 2008).

Um aspecto extremamente relevante, que explica o porquê as crianças e os adolescentes mergulham na imensidade dos espaços virtuais, diz respeito à sensação de controle que estes exercem sobre si mesmos. Assim, acreditam em que não há nada de mais em publicar, por exemplo, uma foto expondo partes do seu corpo ou até mesmo sexualizando. Todavia, esse tipo de postagem atrai os pedófilos e, com base nas informações colhidas, tem condições de se aproximar da vítima e obter sucesso no seu intento.

Outro aspecto importante é que muitas imagens, vídeos e publicações inadequadas, podem influenciar de maneira negativa na formação de crianças ou de jovens, em que a visualização deste conteúdo pode ser internalizada como prática de condutas normais, como exemplo, os vídeos de violência ou até mesmo de pornografia envolvendo práticas sexuais com crianças, animais, entre outros.

Como tudo na vida, temos dois lados, o bom e o ruim. Assim acontece com a Internet, que se mostra uma ferramenta com vasto conteúdo valoroso, basta que seja explorada com responsabilidade e as devidas orientações daquele que possuem mais *expertises* no assunto, fazendo assim com que as chances de ser uma vítima em potencial reduzam drasticamente.

Muitos países do mundo vêm investindo na criação de mecanismo de proteção *online* para crianças e adolescentes, com objetivo de coibir a exposição destes. Todavia, sabemos o quão difícil é ter esse controle, pois apesar das redes sociais não autorizarem a menores de idade, a criação de perfis, isso é facilmente contornado.

O Brasil ainda se mostra muito carente em relação à legislação que trata sobre os crimes praticados por meios virtuais, apesar de termos lei que dispõe sobre o tema – estas, a nosso ver, devem evoluir muito. Por outro lado, nos parece que seria necessária a criação de normas de proteção, quando se tratar do acesso de menores à rede mundial de computadores, incluindo responsabilização aos pais omissos (Pereira, 2015), já que as leis existente sobre a temática são apenas repressivas, isto é, tem efeitos punitivos e não preventivos e educativos.

Findamos assim, com ideia de que a melhor maneira de se resguardar contra os diversos ataques advindos da Internet é a criação de técnicas de prevenção, nas quais podemos orientar nossas crianças e adolescente, para que estas possam explorar o mundo virtual de forma saudável e contributiva para o seu desenvolvimento psíquico intelectual.

3.11 – Resumo do capítulo

A vulnerabilidade mantém-se latente na fase em que pensamos estar prontos para enfrentar todo e qualquer obstáculo da vida. Assim, os adolescentes estão, ao fazer o uso demasiado e sem as devidas orientações das tecnologias conectadas à Internet, tornando-se alvo fácil dos cibercriminosos, os quais acabam por se beneficiar devido a essa autoconfiança encontrada nos jovens.

As ameaças crescem a cada dia, pois muitas são as horas gastas por adolescentes, sejam em função de atividades escolares ou ainda para entretenimento. Neste segundo caso, as redes sociais são as preferidas pelo público adolescente, e é aí que os cibercriminosos se aproveitam para se aproximar destes e evoluir até à prática de delitos, os quais variam do *ciberbullying* até aos mais gravosos, como delitos contra a dignidade sexual ou crimes contra vida, induzindo, instigando ou mesmo levando ao suicídio ou à automutilação, desses adolescentes.

Os riscos das ameaças ciber concretizarem-se, principalmente, com relação aos adolescentes, atingem grandes proporções, na medida em que estamos tratando de uma fase de desenvolvimento psíquico e autoafirmação, onde, muitas vezes, a Internet se torna um ambiente de fuga dos problemas do mundo real, e aí mora o perigo, pois estes podem se tornar ainda mais graves que o imaginado.

É sabido, por todos, que os pais ou os responsáveis têm um árduo dever de cuidados para com suas proles, e esse não se podem limitar somente ao mundo real, mas sim, aos riscos do mundo virtual que, por vezes, é bem maior. Todavia, para atingir esse nível de prevenção, faz-se necessário ganhar a confiança do adolescente, pois a orientação ainda é o melhor caminho, sendo desaconselhada a proibição ou a instalação de programas espiões, já que isso pode causar uma forte barreira entre pais e filhos.

O complemento da educação familiar, sem sombra de dúvidas, é exercido por professores e educadores, os quais passam a conviver com nossos filhos em tempo, muitas vezes, superiores ao que convivemos. Para que essa orientação, sobre os riscos de uma navegação irresponsável pela Internet, possa ser dada, é importante a busca por conhecimento específico por parte dos profissionais que podem auxiliar os responsáveis pelos adolescentes e os próprios adolescentes.

É importante e de grande relevância, o papel na atuação midiática nos dias de hoje, pois esta consegue ter um poder de persuasão sobre a sociedade e tem como recurso a facilidade de propagação da informação para os quatro cantos do mundo. Assim, seria uma forma de conscientizarmos os adolescentes, como o público em geral, sobre os riscos encontrados no ciberespaço e as consequências das ações em contexto digital.

A falta de temor ao acessar a Internet junto à grande quantidade de horas gastas em frente à tela dos computadores, do tablet e dos *smartphones*, faz com que o mergulho no mundo virtual seja de profundidade difícil de prever ou mesmo imaginar. Da simples postagem de uma foto sensual até à participação em desafios perigosos, a obscuridade da rede mundial de computadores traz os mais variados níveis de risco aos adolescentes e, para piorar a situação, o Brasil, ainda tem uma legislação criminal relacionada a cibercrimes muito branda, tendo em consideração as consequências das quais estas vítimas podem sofrer.

CAPÍTULO 4

Os efeitos da Covid19 nas questões de cibersegurança

4.1 – Introdução

No século XXI, o mundo passou a conviver com uma realidade tanto quanto limitada e tenebrosa, fazendo com que as pessoas, mesmo as sem afinidade com a tecnológica, sentissem a necessidade de utilizar os equipamentos digitais, em especial os ligados à Internet. Tais recursos minimizam a ociosidade, facilitando a manutenção das atividades laborais, educacionais e outras.

Inicialmente, discorremos sobre o uso das tecnologias associadas à Internet em tempos de pandemia, em que a potencialização dos serviços *online* e o aumento de horas de acesso à rede mundial despertaram nos cibercriminosos uma oportunidade inigualável de praticarem os seus crimes, tirando partido, muitas vezes, da vulnerabilidade e da falta de conhecimento dos internautas.

A seguir, será tratada a questão da oportunidade criminosa diante deste novo cenário mundial, marcado pela oficialização de uma pandemia. Neste aspecto, faremos uma breve análise de como os cibercriminosos se aproveitaram dos serviços virtuais que passaram a fazer parte do cotidiano das pessoas, para assim colocar em prática os seus ataques cibernéticos e obterem lucros ilícitos.

Posteriormente, iremos expor a oportunidade criminosa diante do novo cenário mundial, já que as pessoas, devido ao isolamento social por conta da pandemia, tiveram a necessidade de recorrer a recursos tecnológicos conectados à Internet para realizar as suas atividades diárias e laborais, tornando-se mais vulneráveis aos cibercriminosos que se aproveitaram do momento para praticar os cibercrimes.

Em continuidade ao assunto, o quarto capítulo fará uma explanação específica sobre um modelo laboral denominado *home office* o qual consiste em obedecer ao isolamento social, fazendo com que os funcionários das empresas trabalhem remotamente das suas próprias

residências. Todavia, mostraremos que, devido ao costume de não praticar protocolos de cibersegurança, acabaram sendo alvos dos cibercrimes, o que trouxe, em muitas situações, prejuízos irreparáveis para as empresas e organizações.

Em seguida, será apresentada uma reflexão sobre a maior vulnerabilidade das crianças e dos adolescentes diante do maior tempo gasto no acesso à Internet em época de pandemia, já que esse excesso, tido como algo normal pelos vulneráveis, pode trazer uma dependência digital e com isso acarretar uma série de problemas, tanto no que diz respeito à saúde mental quanto a integridade física.

No penúltimo capítulo, abordaremos um ponto muito relevante que, por vezes, fica esquecido, qual seja, a vítima sendo considerada culpada pelos cibercrimes sofridos por esta. Mostraremos que a maioria das vítimas de crimes cibernéticos tem participação, porém, não podemos culpá-las por não terem *expertises* suficientes para explorar o mundo virtual.

O sétimo e último capítulo trará ao leitor duas tabelas de protocolos que podem ser utilizados, tanto no âmbito empresarial quanto doméstico, para minimizar as chances de serem alvos de cibercriminosos.

Finalizaremos, com uma reflexão sobre as consequências trazidas pela propagação mundial de um vírus mortal denominado Sars-cov-2, provocando a doença Covid-19, provocada por um coronavírus, que além de causar modificações na vida concreta, trouxe grandes alterações nas atividades desenvolvidas no ambiente virtual, ou seja, no ciberespaço.

4.2 – Uso das tecnologias associadas à Internet em tempos de pandemia

Diante do novo cenário da doença Covid-19, provocada pela propagação do novo coronavírus Sars-cov-2, as pessoas tiveram a necessidade de se adequar às mudanças nas suas vidas, seja no âmbito doméstico, educacional, familiar ou laboral.

A utilização da Internet passou a ser uma ferramenta mais que essencial, devido à proibição de contato físico entres as pessoas. A comunicação virtual ganhou força, de tal

maneira que todas as áreas das nossas vidas foram envolvidas e necessitaram de adaptação, para assim reduzir os prejuízos causados por este vírus, considerado perigoso e mortal.

Ainda devemos destacar que a utilização da Internet no período pandêmico, que atingiu todos os continentes, foi essencial para continuidade do processo de aprendizagem. No entanto, há uma dificuldade em implementar a cultura digital dentro do ensino tradicional, como ferramenta educacional, necessitando de uma reorganização nas práticas pedagógicas. E segundo Santos (2020) "*O ensino a distância vem causando traumas e reatividade a qualquer educação mediada por tecnologias, essa dinâmica compromete sobremaneira a inovação responsável no campo da educação na cibercultura*".

A potencialização da Internet, em especial das redes sociais, trouxe uma série de benefícios para as pessoas, já que estas sentem a necessidade de manter contato umas com as outras. Várias atividades ganharam destaque nesse momento: *lives* virou uma palavra do cotidiano, em que os artistas encontraram espaço para fazer seus shows, políticos fazem campanhas eleitorais, educadores físicos promovem atividades que podem ser realizadas em casa, muitos fazem campanhas solidárias, e uma série de entretenimentos que ajudam a melhorar o fator psicológico e fisiológico dos isolados pela quarentena (Malavé, 2020).

Por outo lado, os meios de comunicações passaram a propagar notícias de caos e de desespero no mundo inteiro, diariamente os noticiários, sejam televisivo ou nas redes sociais, mostraram morte e mais mortes causadas pela Covid-19. E devido a esse excesso de informação, muitos acabaram adquirindo ansiedade e outros transtornos psicológicos. Ainda podemos destacar a desinformação, que leva à descrença da ciência, com relação ao conhecimento epidemiológico, assim como, das orientações sanitárias, trazendo ainda mais riscos para a população.

Aproveitando-se do intenso fluxo que a rede mundial de computadores está produzindo graças a este novo contexto vivido em tempo de pandemia, as atenções dos cibercriminosos voltaram-se ao cometimento de crimes praticados com auxílio de recursos e de equipamentos tecnológicos, fazendo, neste momento de crise, vítimas pelo mundo inteiro.

Devido ao desespero das pessoas e à ansiedade em saber como se encontra o cenário pandêmico, tanto mundial como regional, os malfeitores começaram a criar sites contendo *fake news* (notícias falsas) e disponibilizar aplicativos que tinham como proposta, mostrar mapas

virais, porém, por traz destes pequenos programas, disponíveis para *download*, encontravam-se os *malwares*, responsáveis pela captura de diversos tipos de dados pessoais (Domingues, 2020).

As conferências por meio de vídeos passaram a ser utilizadas para encurtar o distanciamento entre as pessoas, e por isso aumentou a utilização de plataformas, como por exemplo, o *Zoom*, o qual foi vítima dos cibercriminosos, que descobriram falhas e tiveram acesso aos dados de milhões de usuários.

No Brasil, temos a lei 13.709/18 (Lei Geral de Proteção de Dados) que teve sua redação alterada em agosto de 2019 (Brasil, 2018). Esta aborda o tema e prevê punições administrativas às empresas que não tomarem cuidados necessários para proteção dos dados de seus usuários. Tal objetivo é trazido no artigo primeiro desta lei, dispondo

> Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Inferimos que a tecnologia foi e está sendo uma aliada fundamental para a continuidade das atividades cotidianas, porém, as pessoas precisam se conscientizar de que o mau uso destas ferramentas pode trazer prejuízos irreparáveis, sejam eles patrimoniais ou até mesmo psicológicos.

4.3 – Oportunidade criminosa diante do novo cenário mundial

Antes mesmo de virar uma pandemia, o mundo ficou sabendo que um vírus mortal tinha se iniciado na China, e, logo, os internautas começaram a buscar informação nos mecanismos de buscas sobre o assunto. Assim, os cibercriminosos já começaram a se preparar para os seus ataques, com base nos interesses mostrados pela população nas suas pesquisas.

É de importante destaque que, com o confinamento familiar que fora iniciado, o número de delitos contra o patrimônio e até o comércio de drogas ilícitas teve uma considerável

diminuição. Contudo, este novo modelo de vida criou um refúgio virtual, ou seja, o ambiente cibernético, o qual possui as suas virtudes e seu lado sombrio.

De acordo com o IBGE (Instituto Brasileiro de Geografia e Estatística), atualmente, existem, aproximadamente, 220 milhões de *smartphones* ativos no Brasil, tendo em consideração a população Brasileira ser cerca de 211 milhões de habitantes. Aproveitando esta escala, alguns serviços começaram a ser operados de forma mais comum, como por exemplo, os aplicativos de *delivery* – entrega rápida em casa (Rahal, 2020).

Tais aplicativos despertaram os criminosos para atraírem as suas vítimas de modo que estas forneçam os dados dos seus cartões de crédito, juntamente com as senhas, utilizando-se da técnica denominada *Phishing* (Belcic, 2020). Este tipo fraude também é utilizado na emissão de boletos falsos, fazendo com que os usuários acreditem no pagamento real de determinado produto ou serviço, no entanto, o valor é enviado para uma conta desconhecida.

A técnica de *Phishing* conta com ajuda de uma outra denominada *Pharming* que consiste em direcionar o usuário para um *site* falso, porém se mostrando como uma cópia fidedigna do site original. Assim, pensando que está acessando o site verdadeiro, o usuário inseri os dados pessoais relacionados a sua conta, e tem estes subtraídos.

Ainda neste diapasão, um fator de muita relevância foi o alto número de empresas decretando falência e outras reduzindo drasticamente o seu quadro de funcionários. Assim, o número de pessoas desempregadas cresceu e os malfeitores aproveitaram para atrair e subtrair dados destas, por meio de *links* que levavam a sites com falsas propostas de empregos, fazendo com que fossem preenchidos formulários com dados pessoais, os quais seriam furtados.

O *blog* oficial da *Google* reportou que foram enviados mais de 240 milhões de mensagens de *spam* diariamente, contendo em seu texto a palavra COVID, e estes, muitas das vezes, direcionavam os usuários para as 42 mil *web sites* criados do início ao fim do mês de março (gráfico a seguir), que utilizam a mesma técnica referida anteriormente para capturar dados, ilegalmente.

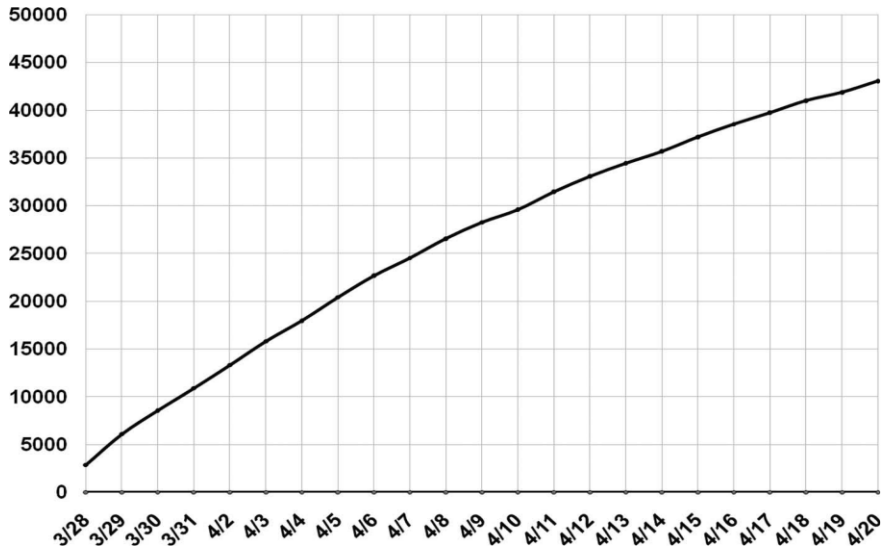


Figura 2 - Número acumulado de domínios relacionados a COVID que foram registrados.

Muitos foram os esquemas de fraude empregados pelos cibercriminosos, tendo como característica o momento de desespero vivido pelo mundo em uma busca frenética pela vacina. Assim, os delinquentes solicitavam contribuições dos internautas para que fosse possível a criação da vacina contra a Covid-19, o que na verdade não passava de artifícios fraudulentos (Jesus, 2020).

Outro recurso que passou a ser utilizado para negociações de produtos é o denominado e-*commerce*, no qual as pessoas anunciam vendas das mais variadas coisas. Aproveitando-se dos dados inseridos nestes sites, os delinquentes conseguem, através de engenharia social, ludibriar as vítimas para fornecerem códigos que são enviados para seu celular, fazendo assim com seu aplicativo *WhatsApp* seja clonado, dando início, ao delito de estelionato, já que passam a solicitar dinheiro aos contatos, induzido a vítima em erro, pois se faz passar pelo proprietário daquela conta.

Em decorrência da falta de *expertise* dos usuários da Internet, a técnica de engenharia social consegue obter o sucesso de 80% dos golpes que são aplicados. E a pandemia, sem sombra de dúvidas, promoveu a oportunidade ideal para os cibercriminosos agirem, fazendo com que houvesse o crescimento significativo de cibercrimes (Naidoo, 2020).

Deduzimos que, após a decretação da pandemia, pela OMS (Organização Mundial de Saúde), as pessoas passaram a utilizar com maior frequência e até de maneira desenfreada, as tecnologias, em especial às conectadas à Internet, já que a comunicação e o contato físico se tornaram perigoso e até mortal. Assim, as barreiras do distanciamento e do isolamento social

foram minimizadas pelas comunicações virtuais. Todavia, junto a este recurso, vieram as problemáticas, tendo como destaque, o aumento da ocorrência de cibercrimes.

4.4 – Os riscos do *home office* para os usuários sem *expertise* tecnológicas

As empresas de pequeno e de médio porte foram as que mais sofreram com o anúncio da pandemia, pois para evitar a contaminação entre os seus funcionários, tiveram que tomar medidas urgentes, e, uma delas foi adotar o sistema de trabalho denominado *home office*, que na sua tradução literal seria trabalho em casa ou escritório em casa.

A empresa Kaspersky, por meio de seu gerente de sênior de mídia social da Kaspersky – Brasil, afirma que "*A má notícia é que, toda vez que algo grande acontece, os cibercriminosos aproveitam a oportunidade*", já que os funcionários foram transferidos das empresas ou dos escritórios para as suas residências sem uma proteção adequada para a realização das tarefas por intermédio da Internet (Rodrigues,2020), tornando alvos fáceis de serem afetados pelos *ransomwares* – *malware* que encripta a informação existente num computador e pede um resgate para a sua recuperação (Kaspersky, 2021).

Em análise realizada, o diretor da equipe de pesquisa e de análise global da Kaspersky (2021) na América Latina, declara que

> O que os cibercriminosos fazem é atacar um hospital ou qualquer outra entidade para roubar informação. Mais tarde, a informação é encriptada e ameaçam tornar os dados roubados públicos. Com vergonha e com medo da desconfiança e multas gerados por um incidente de segurança como este, a maioria das organizações cede às chantagens (Kaspersky, 2021).

e ainda acrescenta: "*Esses grupos são responsáveis por ataques a hospitais e organizações de saúde, serviços críticos durante esta pandemia, mas também visam bancos, companhias de seguros, escritórios de advocacia, empresas de contabilidade entre outros e estão aqui para ficar*."

Para os especialistas, estes ataques ocorreram com grande frequência nos países da américa latina, em especial no Brasil, que teve um aumento em torno de 350% no primeiro

trimestre de 2020, e isso se deve ao fator dos maus hábitos de acesso *on-line* corporativos, dos quais, três se destacam: uso de senhas fracas, utilização de programas piratas e falta de aplicação de correções de software.

Além dos ataques de *ransomwares* e *phishing*, temos muitos outros tipos de cibercrimes que podem ser praticados como destruição de dados, fraudes, paralisação de sistemas dentre outros, e segundo relatórios especializados (Ahmad, 2020), estes custarão ao mundo, 6 trilhões de dólares em 2021.

Um outro *malware* muito utilizado é o *keylogger*, que, após ser instalado no computador da vítima, captura as informações digitadas e envia para o e-mail do criminoso, como exemplo recente deste tipo de arquivo infectado com tal programa malicioso, temos o Eeskiri-COVID-19.chm (Regras da Estônia), o qual aparentemente iria mostrar sites que ajudam no combate à COVID-19.

Verificamos que a *expertise* dos cibercriminosos e o oportunismo estão sempre em alerta. Assim, como as empresas visualizaram uma forma de manter seus serviços em funcionamento no período de isolamento social, causado pela pandemia, os delinquentes também aperfeiçoaram as suas técnicas maliciosas. Logo, devemos salientar que os protocolos de cibersegurança devem sempre ser priorizados, antes da implementação de toda e de qualquer atividade que envolva recursos tecnológicos, em especial, os que estão diretamente conectados à rede mundial de computadores.

4.5 – A maior vulnerabilidade das crianças e dos adolescentes diante ao maior tempo de acesso à Internet em época de pandemia

Como tudo teve que se reinventar em tempos de pandemia, a educação não poderia ser diferente. Os professores foram obrigados a utilizar novos métodos de ensino, apesar de, muitos, nunca terem tido contatos com aulas *online*. Por outro lado, os alunos tiveram que se adaptar como um novo modelo de aula, qual seja, aprendizado à distância, o que para muitos é bem difícil aprender assim.

Além das aulas, as crianças e os adolescentes passaram a ter uma carga excessiva de tempo utilizando-se de tecnologias conectadas à Internet e devido ao grande número de informações sobre o vírus mortal, os mais vulneráveis podem adquirir elevado nível de stresse e ansiedade, já que muitos são os conflitos que podem atormentar as suas mentes, podendo, por sua vez, levar a quadros depressivos.

Para o professor e pesquisador Gustavo Lins Ribeiro (Ribeiro, 2020), a Internet com as suas múltiplas atividades pode proporcionar uma experiência boa ou ruim, trazendo a seguinte conclusão,

> A pandemia do coronavírus é a primeira que se vive no tempo *online*. A Internet, com sua multiplicação da capacidade de comunicação capilar, ao mesmo tempo em que propicia uma tomada de consciência global cria uma expectativa e uma paranoia na espera de que os grandes números de doentes e mortos, supostamente definidos de forma milimétrica diariamente, não atinjam com a mesma intensidade os locais em que vivemos (Ribeiro, 2020).

O problema ainda se agrava quando os mais vulneráveis já apresentam saúde mental comprometida, pois assim, aumenta a probabilidade de idealização e de tentativas de suicídio. Vale a pena ressaltar que, o uso excessivo pode trazer alguns transtornos os quais geram dependência, como por exemplo, cyber sexo, *net gaming*, redes sociais e outros.

Outro risco muito iminente é o de ser vítima de *cyberbullying*, em decorrência, especialmente dos adolescentes, de expor as suas imagens com objetivo de reafirmar uma expectativa de reconhecimento perante os outros internautas, e quem sabe conquistar a fama de um digital influencer. Todavia, as críticas e os insultos constantes, podem trazer prejuízos psicológicos e, sem esquecer, a configuração de crimes contra a honra.

A adolescência é uma época de muitas descobertas, e que poderá vir acompanhada de alguns transtornos psicológicos, os quais podem gerar o desejo da automutilação e até mesmo do suicídio, e a Internet, neste momento, vira um terreno fértil para essa idealização. Um exemplo clássico é o desafio que ficou conhecido como a baleia azul, em que os participantes tinham que realizar uma série tarefas (desafios) e a última era o suicídio.

Neste mesmo contexto de desafios *online*, na atual conjuntura da pandemia, no qual o produto álcool em gel ficou conhecido, por ser uma forma de eliminar o vírus, aproveitaram-se assim da situação e criaram o “Desafio álcool em Gel”, em que os participantes faziam vídeos

inalando, bebendo, cuspindo o produto em direção às chamas e até ateando fogo no próprio corpo, ou seja, práticas de extrema periculosidade da saúde e integridade física (Deslandes, 2020).

Por outro lado, os criminosos, utilizando da inocência das crianças, começaram a criar vídeos com personagens de desenho infantil, que se comunicavam de maneira dissimulada e persuasiva para que estes vulneráveis fornecessem os dados de cartões de créditos dos seus pais.

Depreendemos que, as crianças e os adolescentes podem se tornar dependentes do uso de tecnologias, em especial as conectadas à Internet, e que devido ao cenário pelo qual estamos diretamente envolvidos, o isolamento social, associado com as armadinhas dos cibercriminosos, podem trazer prejuízos tantos para os vulneráveis quanto para seus pais.

4.6 – A vítima sendo considerada culpada pelos cibercrimes

No cenário criminoso, a vítima tem importante papel e deve ser alvo de estudo, por esse motivo que temos a vitimologia, a qual se trata de uma ciência que irá estudar o papel da vítima no crime. No contexto dos cibercrimes, é fundamental analisar o comportamento daqueles que foram alvos dos cibercriminosos.

Dentro da classificação de vítimas temos: Vítima completamente inocente ou vítima ideal é aquela que não teve nenhuma participação na ação criminosa; Vítima por ignorância ou vítima menos culpada que o delinquente é aquela que contribui de alguma forma para ocorrência do delito; Vítima tão culpada quanto o delinquente é aquela que sua participação no crime é fundamental, ou seja, ela se torna vítima em razão de ambição, tanto quanto a do criminoso; e Vítima mais culpada que o delinquente ou vítima provocadora é aquela que traz a culpa para si, ou seja, se tornou vítima por culpa quase que exclusiva de si mesmo (Gonçalves, 2020).

No direito penal brasileiro, o comportamento da vítima é levado em consideração no momento da dosimetria da pena que será atribuída ao delinquente. Porém, se a culpa for exclusiva da vítima, não há aplicação de pena, ficando o agente causador, isento (Brasil, 1940).

Conforme já estudado, os usuários da Internet, em especial, adolescentes, tendem a ter comportamentos inadequados com relação algumas condutas, fazendo com que tenha parte da culpa em alguns delitos sofridos. Todavia, não podemos atribuir a culpa exclusiva para a vítima, tendo em vista que o criminoso é outro, e que não se justifica a prática delituosa por um possível "erro" do internauta inexperiente, displicente ou desinformado.

Em muitas modalidades de cibercrimes, porém, não há participação da vítima, já que as suas ações na Internet são corriqueiras, e, em um belo dia, o que parecia um arquivo enviado pelo seu banco, pode ser um *malware* o qual será instalado no seu dispositivo eletrônico, fazendo você se torna uma nova vítima dos cibercriminosos.

Com a pandemia, as redes de comunicações digitais tiveram que se abrir para comportar um maior número de usuários, ou seja, empresas tiveram que disponibilizar o acesso por meio de ferramentas remotas, as quais são ligadas à Internet. Assim, a vulnerabilidade e ampliação dos riscos inerentes aos crimes cibernéticos aumentaram de maneira considerável, e, devido a essa aceleração digital em tempos de propagação da Covid-19, que os desafio relacionados as técnicas de cibersegurança se multiplicaram (Gouveia, 2020).

Com tais aberturas de redes, as vítimas também se potencializaram, pois devido à falta de preparo com este novo modelo de "vida virtual", poucos se preocupam com as questões de segurança digital ou muitas das vezes confiam na estrutura oferecida pelas empresas as quais realizam suas atividades laborais.

Percebemos, então, que, na maioria dos casos de cibercrimes, a vítima tem uma certa parcela de culpa, pois seu comportamento despreocupado no acesso à Internet vem como um verdadeiro presente para os cibercriminosos, os quais estão sempre na espreita, aguardando os desavisados e descuidados internautas. Por outro lado, temos as vítimas que não contribuem para ação criminosos, tendo nos seus casos falhas de segurança dos sistemas utilizados.

4.7 – Protocolo de cibersegurança

A utilização de toda e qualquer tecnologia, em especial, as conectadas à Internet, requerem cuidados essenciais para que esta ferramenta tão útil e prática, não se torne um risco dissimulada em um cenário criminoso.

A cibersegurança, em especial, para os usuários comuns da Internet, nunca pareceu tão importante, até que estes fossem vítimas dos algozes cibercriminosos. E, em se tratando de nível de organizações, sejam públicas ou privadas, esta segurança que era importante, agora é importantíssima e essencial para o pleno funcionamento de suas atividades.

Vamos começar com a proteção dos computadores pessoais que são utilizados para navegar na Internet e desenvolver as atividades cotidianas (pagamentos de contas, pesquisas, aulas *online* e outras). Na tabela a seguir, mostraremos as principais regras de segurança digital.

Software de proteção	Os programas de antivírus e antimalwares devem estar sempre atualizados e prontos a detectar as ameaças.
Engenharia Social	A orientação é a melhor arma contra este tipo de ataque. Então deve ser ensinado que senhas e outros dados pessoais não devem ser passados a ninguém, por meio da Internet.
Protocolo de Educação	Mostra para os usuários, ao menos, os principais tipos e técnicas de ataques utilizados pelos cibercriminosos. Estas vão dos cuidados ao clicar em *links* desconhecidos até a *expertise* de identificar a técnica de engenharia social.
Políticas de segurança	Consiste em criar documentos que tratem das políticas a serem seguidas para manter uma maior segurança. Este vão do monitoramento até auditorias que serão realizadas nos computadores da organização.

Gerenciador de senhas	Muito importante que os usuários tenham senhas distintas para cada sistema acessado, e que essas sejam fortes, ou seja, longa e com diversos tipos de caracteres. E para não esquecer tais, podem se utilizar de programas gerenciadores de senhas.

Tabela 2 – Principais regras de segurança digital

Conforme visto, é de grande importância que as pessoas antes de ingressar no mundo de tecnologias interligadas à rede mundial de computadores, conheçam os principais conceitos de segurança, pois o terreno é muito fértil para os cibercriminosos que se aproveitam exatamente dessa falta de conhecimento para então atingir suas vítimas.

Com relação a protocolos de cibersegurança, que podem ser utilizados pelas empresas neste atual cenário, as quais disponibilizam o serviço de *home office* para seus funcionários, temos uma pequena lista mostrada na tabela a seguir (Abukari, 2020).

VPN (*Virtual Private Network*)	A VPN irá criar um túnel, onde os dados serão criptografados, tornando assim mais difícil de serem decifrados por intrusos.
Autenticação	Importante que todos os sistemas sejam acessados mediante autenticação, exigindo do usuário senhas fortes.
Software de proteção	Os programas de antivírus e antimalwares devem estar sempre atualizados e prontos a detectar as ameaças.
Engenharia Social	Os usuários devem ser orientados a não fornecer senhas e nenhum dado sem ter a real certeza de que estar falando com o suporte técnico real.

Gerenciador de senhas	Importante que as empresas orientem seus funcionários a utilizarem senhas fortes e diferentes para cada sistema acessado, assim, dificultará a ação dos cibercriminosos. Como recurso pode ser utilizado *software* gerenciador de senhas.
Firewall	A importância do uso de sistemas de *firewall*, como forma de evitar a invasão dos computadores, fechando as principais portas de comunicações utilizada pelos sistemas.

Tabela 3 – Protocolos de cibersegurança

Em análise, podemos inferir que, todos passamos a conhecer um novo cenário mundial que foi modificado após anunciada a pandemia, assim, tanto as pessoas como as organizações, públicas ou privadas, tiveram que se reinventar para não entrarem em crise econômica e até a decretação (declaração) de falência. Porém, devido ao curto espaço de tempo que tudo ocorrera, não deu tempo da preparação de pessoal para lidar com um novo método de trabalho, associado com os recursos ligados à Internet.

4.8 – Resumo do capítulo

O mundo teve um grande impacto no ano de 2020, devido à pandemia causada pela Covid-19 e tal situação fez com que os trabalhadores se isolassem em suas casas e executassem os seus trabalhos a partir de computadores conectados à Internet. Mas, não só os adultos, as crianças e os adolescentes, também tiveram alterações aos seus cotidianos, pois passaram a interagir com os professores e os colegas por meios virtuais. Isso tudo trouxe riscos para aqueles que não conhecem e não sabem detectar os possíveis ataques cibernéticos.

Com este crescimento no uso de tecnologias, em especial, conectadas à Internet, os cibercriminosos depararam-se com uma oportunidade imperdível de articularem seus ataques, tendo estes os mais diversos objetivos, os quais vão da propagação de pânico na sociedade, passando pelo furto de dados, crimes contra honra, e podendo ir até à indução de suicídios, pedofilia infantil, entre outros delitos mais gravosos.

Conforme abordada, o *home office* passou a ser uma opção para as atividades que conseguem ser executadas desta maneira. Todavia, tanto funcionários como as próprias empresas, muitas vezes, não estavam preparadas tecnologicamente com *hardware* e *software* específicos para assegurar a segurança da informação. E, junto a isso, vêm a inexperiência e os maus hábitos dos usuários ao acessarem à rede mundial de computadores, tornando-se assim, alvos dos cibercriminosos e colocando em risco dados da empresa, podendo trazer prejuízos irreparáveis e expondo inclusive dados pessoais e informação que consta nos próprios computadores em cada.

O isolamento social atingiu em cheio as crianças e os adolescentes os quais tiveram que aprender a conviver com aulas *online* e com entretenimento virtual, sejam redes sociais, *games*, *sites* de interesse etc., como meio de tentar reduzir a carga de stresse causado pelo confinamento. Todavia, a probabilidade de serem vítimas dos cibercriminosos aumentou significativamente, os quais se utilizam de recursos específicos para captar esse público vulnerável.

Por outro lado, temos, frequentemente, a vítima sendo colocada como culpada por ter sido alvo dos cibercriminosos. Assim, devemos ter cautela em fazermos uma tão difícil análise, pois a participação do ofendido pode ser relevante, porém, em um contexto geral, não podemos vitimá-lo duas vezes. Deve ser levado em consideração que, na maioria dos casos, os ataques são dissimulados e aquele que não tem a *expertise* suficiente, irá certamente cair na armadilha.

Importante, então, usarmos os protocolos mínimos de segurança para, ao menos, identificarmos e escaparmos dos ataques mais comuns. E tais medidas e conhecimentos podem ser obtidos por meio de *sites* confiáveis, que tratam de segurança da informação, e que estão disponíveis na própria Internet. Logo, seguindo esses procedimentos, o usuário conseguirá ser menos vulnerável à ocorrência de cibercrimes.

CAPÍTULO 5

Metodologia

5.1 – Introdução

O presente trabalho tem como objetivo principal, desenvolver uma proposta de modelo que possa auxiliar todos os envolvidos nas questões perigosas de cibersegurança (ameaças) relacionadas com o contexto específico, no que diz respeito ao acesso descontrolado e não supervisionado de tal público (adolescentes) que explore vulnerabilidades existentes, aumentando consideravelmente os riscos de se tornarem vítimas de ações criminosas.

A realidade que nos deparamos nos dias contemporâneos é a de um acesso irrestrito feito pelos adolescentes, que se encontram em fase de autoafirmação e se acham prontos para o enfrentamento da vida, seja, real ou "virtual". Esta segunda vem se destacando e crescendo a cada dia mais, pois em uma era tecnológica muitos jovens ficam reféns e literalmente dependentes dos recursos digitais.

O principal objetivo de escolhermos uma metodologia adequada para a pesquisa é de conhecermos melhor o fenômeno estudado, e para que este seja alcançado, nos valeremos de diversos artigos científicos, de modo a fundamentar o estudo, complementado com a aplicação de questionários e, posteriormente será feita a coleta e análise dos dados obtidos. São apresentados através de gráficos todos os dados da pesquisa, para posterior análise.

Com base em nosso objetivo, verificamos e escolhemos, além da metodologia qualitativa, uma abordagem de investigação-ação, pois essa se baseia em compreender um fenômeno prático e uma possível mudança ou minimização real do problema. Vale ressaltar que, esta metodologia segue os seguintes processos, os quais iremos explorar no decorrer do trabalho, que são: planejamento, ação e reflexão (Abrantes, 2011).

Levando em consideração os processos mencionados anteriormente, podemos esclarecer o que será realizado em cada etapa.

A primeira é o planejamento, onde definiremos o problema que nos propusemos a investigar e estudar de forma aprofundada, nos questionando se vale a pena tal pesquisa, se poderemos obter uma solução, ainda que parcial, e se este trabalho irá contribuir para outras pessoas além do próprio investigador. Vale ressaltar que, após responder a estes questionamentos, se faz importante fazer um referencial do trabalho, onde colocaremos todas as etapas que deverão ser realizadas para concluímos, com êxito, a pesquisa científica que nos dispusemos a desenvolver.

Na segunda fase, qual seja a de ação, iremos colher informação das diversas fontes documentais confiáveis e científicas, além de, fazermos a pesquisa de campo, aplicando questionários para recolha de dados, e em seguida, observarmos tudo o que recolhido e estudado, conforme o planejamento feito anteriormente.

Na última fase, iremos nos dedicar a reflexão onde analisaremos os dados obtidos na nossa intervenção, e em seguida, refletirmos acerca dos dados recolhidos, de maneira crítica, para posteriormente tomar decisões e propor uma possível solução ou redução do problema o qual nos motivou a fazer o estudo.

Finalmente, temos que informar que, está pesquisa será realizada na cidade de Belém no Estado do Pará no Brasil, e que serão escolhidos participantes de forma aleatória que se encaixem no perfil que será estipulado para obtermos um cenário concreto da proposta de tese.

5.2 – A abordagem metodológica qualitativa da investigação

Antes de iniciarmos a colocações a respeito da metodologia qualitativa, a qual foi escolhida, temos que conhecer a etimologia da palavra metodologia vinda do grego Méthodos, que significa direção, caminho, isto é, meio mais eficaz de atingir a meta, objetivo.

De acordo com Oliveira (Oliveira, 2018), metodologia da pesquisa é

> um processo que se inicia desde a disposição inicial de se escolher um determinado tema para pesquisar até a análise dos dados com as recomendações para minimização ou solução do problema pesquisado. Portanto, metodologia é um

> processo que engloba um conjunto de métodos e técnicas para analisar, conhecer a realidade e produzir novos conhecimentos (Oliveira, 2018).

O uso da metodologia qualitativa nesta tese, se dar pela flexibilidade que esta dispõe, especialmente relacionada a técnica de colheita de dados, a qual poderá utilizar questionários, pesquisas anteriores e, até mesmo a observação.

A característica que irá marcar esta pesquisa é a análise e a integração de informações trazida pela variedade de material recolhido pelo pesquisador, que vai utilizar a sua capacidade indutiva e criadora (Martins, 2004).

Por último, devemos deixar bem claro que, o método qualitativo é utilizado para estudar diferentes grupos sociais, e nossa proposta é exatamente estudar o grupo dos adolescentes e demonstrar através de análise de documentos e dados coletados em questionário que, a vulnerabilidade, com relação aos cibercrimes, pode ser mitigada a partir do momento em que existir uma espécie de força tarefa à qual envolve diversos personagens, como os responsáveis legais, os professore e educadores, a mídia e o próprio Estado.

5.3 – Investigação-ação

O trabalho de investigação empírica contou com a utilização da metodologia de investigação-ação. Tendo em consideração que "*é difícil definir a Investigação-acção por duas razões interligadas: primeiro, é um processo tão natural que se apresenta, sob muitos aspectos, de diferentes modos e, segundo, que se desenvolveu de maneira diferente para diferentes aplicações e contextos*" (Tripp, 2005).

Ainda de acordo com Tripp, temos os seguintes ciclos da investigação-ação:

- A pesquisa-ação começa com um reconhecimento. O reconhecimento é uma análise situacional que produz ampla visão do contexto da pesquisa-ação, práticas atuais, dos participantes e envolvidos. Paralelamente, a projetar e implementar a mudança para melhora da prática, o reconhecimento segue exatamente o mesmo ciclo da pesquisa-ação, planejando como monitorar e avaliar a situação atual e, a seguir, interpretando e

avaliando os resultados, a fim de planejar uma mudança adequada da prática no primeiro ciclo de pesquisa-ação de melhora;

- Pesquisa-acção num ciclo iterativo: a natureza interativa do processo de Investigação-acção talvez seja sua característica isolada mais distintiva. Muito embora todos os processos de melhoria e desenvolvimento tendam a incluir todas as fases do ciclo básico de Investigação-acção, nem todos o fazem na mesma sequência, nem repetem o ciclo de uma maneira constante para realizar melhorias de modo incremental. A maioria das soluções de problemas, por exemplo, no caso do desenvolvimento organizacional ou da pesquisa experimental, não constituem Investigação-acção, segundo esse critério. A pesquisa-acção, como uma forma de Investigação-acção, é um processo corrente, repetitivo, no qual o que se alcança em cada ciclo fornece o ponto de partida para mais melhoria no ciclo seguinte.

Encontramos a definição dada por outro autor, que assim se expressa "*aprender fazendo, em que é identificado um problema, se faz algo para o resolver e se verifica se os esforços resultaram. (...) Sendo esta a essência deste método, possui uma série de atributos que o diferenciam de uma simples resolução de problemas*" (Alfredo, 2014):

- Assume-se um duplo compromisso em estudar um sistema e introduzir-lhe alterações naquela que é a direção desejada;
- Implica o envolvimento do investigador participante numa aprendizagem conjunto;
- A ênfase é colocada no estudo científico, sendo o problema tratado de forma sistemática e com um corpo teórico que sustenta as intervenções dos participantes;
- Combina o diagnóstico com a reflexão, focando-se em problemas reais que foram identificados pelos participantes como problemática, mas passíveis de serem alterados.

Acrescentando, o mesmo autor ainda traz que, a Investigação-acção é "*uma metodologia que permite a ligação efectiva e eficiente entre a investigação e a sua aplicação em termos práticos no processo educativo. O objectivo final é de obter respostas que sejam aplicáveis na prática diária dos intervenientes e que possam ser transmitidas a outras pessoas interessadas*".

Em uma das abordagens o autor considera que o modelo de Investigação-ação possui as seguintes etapas (Alfredo, 2014):

- Identificação, avaliação e formulação de um problema;

- Apresentação de propostas/sugestões por todos os participantes e análise delas;
- Pesquisa bibliográfica sobre o problema;
- Reformulação do problema, se necessário, apresentação de hipóteses;
- Escolha dos procedimentos a aplicar;
- Escolha dos tipos/mecanismos de avaliação a utilizar;
- Implementação/activação do projecto;
- Observação e avaliação dos resultados obtidos e a tomada de consciência das implicações dos mesmos.

O caso trabalhado nesta pesquisa científica, permitiu extrair informação relevante para obtenção de conhecimento, suficiente, para entender como as questões de cibercrimes e cibersegurança são percebidas pelos pais ou responsáveis legais, podendo, assim, caminhar rumo ao descrito na proposta inicial que, é a produção de uma cartilha de orientação e prevenção contra os delitos cibernéticos.

5.3.1 – Amostra

Este estudo irá envolver informações relacionadas aos pais ou responsáveis legais, bem como dos adolescentes, aqueles que possuem entre 12 e menos de 17 anos de idade. E como amostra, iremos retirar dados que estão diretamente ligados à cibersegurança, levando em consideração uma premissa que é a prevenção contra cibercrimes, isto é, aqueles praticados em ambientes virtuais que podem ou não passar para o ambiente real.

Participaram desta pesquisa 200 pessoas, por meio de respostas feitas em um formulário, *online* e, alternativamente, por recurso a papel, manualmente, de um conjunto de questões sobre a temática proposta nesta tese cibersegurança e uso da Internet/Web.

5.3.2 – Procedimentos

Ainda antes de reportar a recolha de dados, passamos por uma fase inicial de reunir vários artigos científicos, que fizeram com que o estudo fosse iniciado com a apresentação da rede mundial de computadores, partilhando conceitos importantes para compreender o impacto do digital nos delitos. Foram, igualmente, introduzidos os conceitos de cibercrimes, cibersegurança e as suas ramificações.

Em um segundo momento foi reportada a vulnerabilidade de adolescente, face aos cibercriminosos, já que este é o público-alvo da pesquisa. Neste contexto, foram apresentadas as principais características da fase da adolescência, assim como, o importante papel dos pais ou responsáveis legais, dos profissionais que lidam com esses adolescentes, do governo e da mídia, no auxílio ao combate aos cibercrimes. Tal posição, revela a convição da importância da prevenção, colocando em prática as orientações de cibersegurança e evitando assim que os adolescentes mais vulneráveis sejam vitimados pelos cibercriminosos – num claro processo de mitigação por via da prevenção.

Numa terceira fase, partimos para a recolha de dados, com o objetivo de verificação e análise e para entendermos o fenômeno estudado. Nomeadamente, para a comprovação se há ou não falta de conhecimento sobre o tema cibersegurança, e o quanto pode ser importante uma cartilha de orientação para suporte à prevenção das vulnerabilidades dos adelescentes no uso e exploração da Internet/Web.

5.3.3 – Instrumentos

Os instrumentos utilizados foram os questionários, com recurso ao *Google Forms*. O questionário contém várias perguntas, de modo a verificar o comportamento dos adolescentes ao acessarem à Internet, bem como o conhecimento e os cuidados dos pais ou responsáveis legais.

5.4 – Pesquisa Documental

Primeiramente, temos que partir do conceito de documentos, e nos utilizaremos da etimologia da palavra que, significa aquilo que serve de exemplo, que ensina. O conceito de documentos é (Cellard, 2008)

> tudo o que é vestígio do passado, tudo o que serve de testemunho [...] pode tratar-se de textos escritos, mas também de documentos de natureza iconográfica e cinematográfica, ou qualquer outro tipo de testemunho registrado, objetos do cotidiano, elementos folclóricos (Cellard, 2008).

A pesquisa documental é aquela que se utiliza de documentos vindo de fontes primárias, isto é, que não receberam nenhuma forma de tratamento analítico. Assim, é uma abordagem de pesquisa que utiliza, exclusivamente, ou, em complemento, dados provenientes de documentos, com a finalidade de extrair informação neles contidas, objetivando compreender determinado fenômeno, após uma análise (Kripka, 2015).

A recolha documental e a consecutiva extração de informações foi realizada em diversos documentos da literatura voltada aos estudos em tecnologias da informação, psicologia, sociologia, metodologia entre outros que abordam o tema da cibersegurança e do público em estudo: os adelescentes. Procedeu-se assim à leitura de artigos, livros, teses de doutoramento e dissertações de mestrado, o que permitiu o desenvolvimento do estado da arte que compôs o referencial teórico da investigação proposta na tese.

Nesse sentido, temos um envolvimento cooperativo e participativo do investigador com a temática da pesquisa, o qual, irá contribuir para propor ações ou resoluções de problemas com que a comunidade é confrontada.

Foi neste contexto que, se procedeu à exploração documental dos temas que envolvem de um modo geral a vulnerabilidade de adolescentes à cibercrimes, bem como, à proposta de mitigação das ocorrências por meio de cibersegurança na comunicação preventiva.

5.5 – Recolha de Dados e Análise do Questionário

A recolha de dados será feita por meio de questionário, disponibilizado na plataforma *Google Forms* e/ou impresso e entregue ao participante da pesquisa, o qual deverá, primeiramente, ler as instruções iniciais e concordar com a participação voluntária, e, logo em seguida, preencher o questionário o qual conterão perguntas objetivas e subjetivas. O uso de uma versão manual do questionário constitui uma alternativa de modo a garantir a recolha de dados, mesmo em casos de menor literacia tecnológica ou dificuldades pelos pais ou responsáveis legais do adolescente, já que o questionário lhes era dirigido. Deste modo, são ultrapassados desvios de seleção de respondentes apenas com maiores competências digitais.

Em caso de aplicação por meio do *Google Forms*, o *link* para os participantes foi enviado via correio eletrónico, que os direcionou para o site com as instruções para que possa fazer o preenchimento de forma fácil, prática e autônoma.

Após preenchidos 200 questionários com participantes que possuem filhos ou menores, adolescentes, que estão sob sua responsabilidade legal, será colocado em planilha eletrônica e consequentemente montado gráficos para melhor mostrar os resultados (importa registrar que cada questionário contem as respostas para apenas um filho adolescente, de modo a garantir uma relação de um para um, entre questionário e adolescente).

Com base nos resultados obtidos, partiremos então para a aplicação da nossa proposta de comunicação mais segura para os adolescentes que ingressam no mundo virtual que, sem serem orientados pelos responsáveis, se possam tornar vulneráveis e vítimas em potencial dos cibercriminosos.

Vale ressaltar que, as perguntas realizadas não permitem identificar de nenhuma forma os participantes da pesquisa e que, os dados extraídos serão utilizados, exclusivamente, para a proposta desta tese de doutoramento, estando garantidos os tramites legais e de enquadramento com dados de acordo com a lei de proteção de dados e os necessários procedimentos associados com a comissão de ética/Plataforma Brasil.

5.5.1 – Justificativa da escolha dos participantes

O pesquisador optou em fazer o questionário direcionado aos pais ou responsáveis legais dos adolescentes, pois estes tem o dever legal do cuidado para com o seu adolescente. Logo, é necessário que quem tutela os adolescentes, possua conhecimento, ainda que básico, sobre cibercrimes e cibersegurança, a fim de orientar de maneira correta os seus e assim, evitar que sejam alvos dos criminosos que agem na Internet.

Não escolhemos fazer a entrevista com os próprios adolescentes por dois motivos principais. O primeiro é que devido a terem proteções diferentes, teríamos mais dificuldades na recolha de dados, e depois eles se encontram em uma fase que tendem a omitir ou mentir sobre as questões que lhes são colocadas, ainda mais, em um tema que podem considerar como de foro íntimo. Logo, não seria interessante a colheita desses dados para nossa pesquisa científica.

As opções de realizar um formulário na plataforma disponível pelo *Google Forms* é a de que a maioria das pessoas possuem *smartphones* como o seu celular (telemóvel), o que facilita o preenchimento de forma fácil e prática.

A possibilidade de imprimir os questionários, foi tomada devido ao pesquisador ser professor e lidar com alunos adultos que são pais de adolescentes, fazendo com que tenha facilidade de solicitar a colaboração destes para a sua pesquisa.

Estas foram as justificativas que nos levaram aos procedimentos tomados para a recolha e posterior análise de dados.

5.5.2 – Divisão da pesquisa em grupos

Ao produzirmos as perguntas, fizemos subdivisões, primeiramente definimos quais questões que estariam relacionadas com os adolescentes e aquelas voltadas para os responsáveis. Assim, determinamos que as perguntas de 1 a 6, e, de 11 a 15, tratam de informações relacionadas aos adolescentes. Por outro lado, temos os questionamentos de 7 a 10, e, de 16 a 21, ligadas aos responsáveis.

Ainda dividimos as questões por grupos para melhor trabalhar as questões: o grupo de número 1 é formado pelas perguntas 1 a 3 que, caracterizam o adolescente, fazendo questionamentos sobre idade, gênero e escolaridade.

O grupo número 2, com as perguntas 4 a 6, com o objetivo de colher as questões de conectividade, isto é, se o adolescente possui dispositivo que se conecta à Internet, bem como, se possui conta em rede social ou acesso a rede social dos seus responsáveis.

O grupo número 3, com as perguntas 7 a 10, que mostram a caraterística pessoal e específica dos responsáveis frente ao acesso dos seus filhos, isto é, questionando sobre o conhecimento das publicações feitas pelo adolescente, bem como saber quem são os contatos virtuais destes e, se há monitoramento, incluindo, também, a escolaridade do responsável.

O grupo número 4, responsável por questionamentos relacionados aos hábitos digitais, composto pelas questões 11 a 15, que permitem extrair o tempo de conectividade, as atividades extraescolares, conhecimentos sobre se o adolescente possui grupo de amigos que se encontram fisicamente, e ainda, se esses adolescentes costumam sair para socializar ou se ficam nos seus quartos, utilizando os seus dispositivos ligados à Internet.

O último grupo, número 5, tem por objetivo extrair a consciência que o responsável tem em relação ao tema cibercrimes e cibersegurança, colocando perguntas conceituais e genéricas sobre o tema. Adicionalmente, indaga sobre a atitude que devem ter e qual a delegacia procurar no caso em que o adolescente venha a ser vítima de cibercriminosos. Por último, são realizadas perguntas relacionadas com a opinião dos responsáveis no que diz respeito à maior propagação e discussão do tema, tanto nas escolas como nos meios de comunicação oficiais, incluindo a pergunta chave do nosso questionário, que é o interesse de receber uma cartilha de instruções e orientações para prevenção dos cibercrimes, voltados, especialmente, para os adolescentes.

Inferimos que, estas subdivisões nos ajudam a melhor cruzar os dados e fazer diversas análises, as quais nos podem proporcionar diversas contribuições úteis para a elaboração da cartilha, principal contributo pretendido para este trabalho de investigação.

5.6 – Questionário aplicado aos responsáveis dos adolescentes

Será repassado um questionário para que os responsáveis dos adolescentes possam responder e, assim, fazermos uma análise e extrairmos as informações que contribuem para a elaboração de uma cartilha de prevenção aos cibercrimes que vitimizam este público.

5.6.1 – Informações para os participantes

Leia atentamente as informações antes de começar a responder o questionário, com objetivo de participar do estudo o qual trata esta tese de doutoramento. Por favor, responda às perguntas objetivas relacionadas ao projeto antes de completar seu consentimento. Ainda destacamos, a importância de as respostas serem respondidas com sinceridade, a fim de que possamos fazer uma análise final e com base nela possamos desenvolver uma proposta a qual será de grande contribuição para a sociedade de modo geral.

Você está sendo convidado a participar voluntariamente, e caso queira desistir de prossegui respondendo o questionário, poderá fazer a qualquer momento, antes de finalizar o processo. Porém, saiba que a sua participação é muito importante para nossa pesquisa de doutoramento, já que elas farão parte do capítulo de análises e conclusões.

Manteremos a confidencialidade e não terá nenhuma pergunta relacionada aos seus dados pessoais, mas, tão somente as que interessam para o estudo dos dados. E após análise desses dados, a publicação da pesquisa empírica poderá ocorrer em revistas científicas, *sites* acadêmicos, apresentações presenciais, *sites* de publicações de artigos dentre outros.

ATENÇÃO: **PARTICIPANTE PRECISA ACEITAR TODOS OS REQUISITOS DE VOLUNTARIEDADE E CONCORDÂNCIA, CASO CONTRÁRIO SUAS RESPOSTAS NÃO SERÃO UTILIZADAS NA ANÁLISE DA PESQUISA CIENTÍFICA.**		
Li atentamente as informações para os participantes	☐ SIM	☐ NÃO
Entendo que minha participação e voluntária e que posso desistir de continuar respondendo às perguntas, desde que seja antes de enviar a resposta e que meus dados serão utilizados com finalidade de estudos científicos e nada mais.	☐ SIM	☐ NÃO
Eu aceito que os dados coletados serão publicados em sites, artigos e apresentados na defesa da tese.	☐ SIM	☐ NÃO
Eu aceito participar desse estudo científico.	☐ SIM	☐ NÃO

5.6.2 – Questionário

Após preenchidos as informações referentes à participação voluntária e com a certeza de que os dados serão usados exclusivamente com objetivo acadêmico de contribuir com a ciência e a sociedade, são apresentadas as 21 (vinte e uma) questões do questionário:

1. Que idade tem o adolescente? ☐ ANOS
2. Qual o gênero do adolescente? ☐ MASCULINO ☐ FEMINIMO
3. Que ano/curso frequenta o adolescente? 1º GRAU ☐ 2º GRAU ☐ CURSO ☐
4. O adolescente possui acesso à dispositivos conectados à Internet (smartphone, tablet, computador etc.)? ☐ SIM ☐ NÃO

5. O adolescente possui alguma rede social (Facebook, Instagram, WhatsApp etc.)? ☐ SIM ☐ NÃO
6. O adolescente possui acesso às suas contas em rede social? ☐ SIM ☐ NÃO
7. O responsável está ligado ou tem acesso às publicações nas redes sociais do adolescente? ☐ SIM ☐ NÃO
8. Qual a escolaridade do responsável? ☐ FUNDAMENTAL ☐ MÉDIO ☐ SUPERIOR
9. O responsável faz o controle desse acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal? SIM ☐ NÃO ☐
10. O responsável conhece todos os contatos virtuais do adolescente? ☐ SIM ☐ NÃO
11. Quanto tempo em média o adolescente fica conectado à Internet?
12. O adolescente possui atividades extraescolares ou desporto, de forma frequente? ☐ SIM ☐ NÃO
13. O adolescente possui um grupo de amigos regulares com quem se encontra fisicamente? ☐ SIM ☐ NÃO
14. O adolescente sai de casa de forma regular para ir a locais além da escola, para socializar? ☐ SIM ☐ NÃO
15. O adolescente usa computadores ou smartphone no seu quarto? ☐ SIM ☐ NÃO
16. O responsável sabe o que é cibercrime? ☐ SIM ☐ NÃO

17. O responsável tem conhecimento que o adolescente já foi vítima de algum cibercrime? ☐ SIM ☐ NÃO
18. O responsável sabe a que Delegacia de Polícia Civil Especializada a qual deve recorrer caso do adolescente seja vítima de cibercrimes? ☐ ☐ SIM NÃO
19. O responsável acha importante as escolas abordarem tema como o cibercrime e a cibersegurança? ☐ SIM ☐ NÃO
20. O responsável acha importante a divulgação sobre cibercrimes e cibersegurança nos meios de comunicações oficiais? ☐ SIM ☐ NÃO
21. O responsável gostaria de ter acesso a uma cartilha de instruções que mostra os principais cibercrimes e o modo de prevenção, voltado, especialmente, aos adolescentes? ☐ SIM ☐ NÃO

Com base nos dados recolhidos, poderemos ter uma visão da realidade enfrentada quando ao assunto da cibersegurança, considerando os adolescentes e, na perspetiva dos seus responsáveis legais. É nossa convicção que o adolescente necessita de proteção e principalmente orientação para reduzir as chances de ser vítima em potencial dos cibercriminosos e dos seus atos.

5.6.3 – Por que das perguntas do questionário?

Em primeiro lugar, é necessário saber a idade do adolescente, tendo em vista que há diversas fases deste período vital, e assim, permitir fazer uma análise mais geral a qual possa abranger a cibersegurança de toda faixa etária da adolescência (dos 12 aos 17 anos),

A segunda pergunta é para que possamos fazer um comparativo dos cuidados que os responsáveis têm quando de se trata de adolescente do sexo masculino ou feminino, verificando se há diferenças.

O terceiro aspeto pretende analisar com o questionamento relacionado com a escolaridade e, para se sentir a questão de possível orientação ou até mesmo cuidados quando se está acessando a Internet.

O quarto quesito, analisa e possibilita obter o percentual de adolescentes que possuem ferramentas que permitam a coneção à rede mundial de computadores.

O questionamento seguinte, pretende apurar o quantitativo de adolescentes que possuem redes sociais, as quais, são consideradas ferramentas facilitadoras perfeitas para a prática de determinados cibercrimes.

Em seguida, continuamos o questionário perguntando se os pais, por algum motivo, fornecem senhas das suas próprias redes sociais. A importância desta pergunta é exatamente para saber o grau de confiança estabelecido em adolescentes e responsáveis.

O sétimo questionamento, visa saber se o responsável conhece as publicações feitas pelo adolescente, com a intenção de saber qual é caminho que este está pretendendo trilhar com as suas preferências, as quais, são externadas na forma que se apresentam para os pares, por meio de postagens na rede.

O questionamento de número oito, tem por objetivo, saber o grau de escolaridade dos pais ou responsáveis e, relacionar este, com o conhecimento sobre a temática estudada.

Em continuidade ao raciocínio, temos interesse em saber se os responsáveis possuem algum tipo de controle sobre o acesso do adolescente, seja por meio de programas que limitam esse acesso, ou por monitoramento pessoal, isto é, verificando de tempo em tempo as atividades realizadas pelo adolescente na Internet.

A décima pergunta, tem objetivo de identificar se os responsáveis monitoram o ciclo de pessoas que o adolescente se comunica nas redes sociais, e ainda, de que grupos faz parte, que tipo de ideologias seguem, etc.

A pergunta onze, tem por finalidade, saber a quantidade de horas o adolescente passa conectado à Internet, diariamente. Assim, podemos tirar conclusões como, por exemplo, a chance deste ser vitimizado por cibercrimosos.

O questionamento posterior, tem uma ligação com a terceira pergunta, justamente para saber se o adolescente gasta o seu tempo com outras atividades extraescolares, fazendo com que seja reduzido o seu tempo de permanência na Internet.

A décima terceira pergunta, visa saber se o adolescente partilha o seu tempo com atividades reais (não digitais), isto é, socializando com outros colegas e procurando interagir fisicamente com estes, ao invés de simplesmente ser interação virtual.

Em sequência, procuramos saber se o adolescente frequenta locais diferente da escola, para socialização com as pessoas que ali estão.

O quesito seguinte é de extrema relevância, tendo em mente que, o perigo no isolamento aumenta significativamente, já que o adolescente se sente à vontade em realizar toda e qualquer conduta, pois tem a privacidade e reserva do seu quarto, ficando assim, mais difícil o monitoramento por parte dos responsáveis.

A décima sexta pergunta, está relacionada diretamente com os cibercrimes, querendo ter uma visão mais ampla de que, o responsável tem conhecimento dessa modalidade criminosa.

Em seguida, mas no mesmo panorama, queremos saber se o responsável tem conhecimento de que seu filho já foi alvo de alguma espécie de cibercrimes.

No décimo oitava quesito, se pretende saber se os responsáveis têm ao menos o conhecimento básico para recorrer a autoridade competente e específica, caso o adolescente que está sob seus cuidados, venha a ser vitimado pelos cibercriminosos.

Nos quesitos finais, como é o caso do décimo nono, pretendemos dos responsáveis qual o interesse em ter o tema da cibersegurança abordado nas escolas.

Em continuidade ao raciocínio anterior, a pergunta que se segue, pretende indagar sobre o quanto é importante a propagação do tema em debate, nas mídias de comunicação oficial.

Finalmente, e com objetivo de avaliar a relevância da contribuição desse estudo para com a sociedade, é questionado se o responsável gostaria de receber uma cartilha expliclativa, mostrando os principais crimes praticados por intermédio da Internet e o meio pelo qual se pode prevenir, reduzindo, assim, a chance de o adolescente se tornar uma vítima de cibercrimes.

5.7 – Divisão em grupos de questões

Após a aplicação do questionário, dividimos as perguntas em grupos, onde obtivemos 5 (cinco): identificação, conectividade, caracterização, hábitos digitais e consciência. Em cada grupo foram colocadas entre 3 (três) e 6 (seis) perguntas que estão diretamente ligadas a denominação dada a estes.

O grupo de identificação é composto por 3 (três) perguntas que visa conhecer a caracterízação do adolescente, questionando a sua idade, gênero e escolaridade. Assim, poderemos fazer análises que nos mostrem se esse conjunto de informação tem relação direta com as questões de vulnerabilidade e conhecimento sobre os riscos de serem vítimas de cibercriminosos.

No grupo de conectividade encontramos 3 (três) questões que permitem mostrar a relação desses adolescentes com a Internet, de modo a que saberemos se possuem acesso à rede mundial de computadores e se de alguma forma utilizam redes sociais, seja de forma pessoal ou acessam às dos seus pais ou responsáveis legais.

Na caracterização, formada por 4 (perguntas) que compõem o grupo 3 (três), procuramos obter informação sobre os pais ou responsáveis no que diz respeito ao controle, monitoramento e conhecimento das práticas realizadas pelo seu filho ao acessarem à Internet. Adicionalmente, foi questionado o grau de escolaridade dos responsáveis, para então, analisarmos se há alguma ligação com a questão dos cuidados para com seus adolescentes, isto é, se o grau de escolaridade mostra conhecimento sobre tecnologia e, principalmente, sobre os riscos que esta possui por conta de cada de acesso realizado.

Uma parte do questionário diz respeito ao grupo 4 (quatro) de questões que, possui 5 (cinco) perguntas relacionadas com a forma como os adolescentes utilizam a tecnologia ligada à Internet. Assim, podemos analisar os hábitos de acesso, extraindo informação relacionada ao tempo médio de uso, a questão de socialização com pessoas, a prática de frequentar lugares diversos da escola e até mesmo fazer atividades desportivas, e finalmente, se utilizam lugares reservados, como o quarto, para terem acesso mais privativo e sem estarem à vista e controle dos seus responsáveis legais. Logo, este grupo mostrará o quão vulnerável é o adolescente,

incluindo os problemas físicos e psicológicos daqueles que dedicam a maior parte do seu tempo em frente a uma tela de um computador ou *smartphone*.

Finalmente, no grupo 5 (cinco), são realizadas questões que irão justificar a nossa pesquisa, tendo em vista o conhecimento dos participantes sobre os assuntos associados com os cibercrimes e a cibersegurança. Assim, fizemos perguntas relacionadas com estes temas, verificando o interesse em ter um material que posso auxiliar a compreender os males que a rede mundial pode trazer e como se prevenir, tendo em consideração, os problemas de natureza física e psicológica que podem afetar o adolescente e, de forma grave, já que estes se encontram em uma fase de desenvolvimento físico e mental.

5.8 – Resumo do capítulo

No capítulo voltado para a exposição da metodologia, falamos, primeiramente, sobre o método qualitativo de investigação e, depois da Investigação-ação.

Recorreu-se a uma metodologia, além da qualitativa, da denominada Investigação-ação, a qual se enquadra na presente pesquisa, já que se organiza em etapas que fazem parte da nossa estrutura de trabalho, são elas: Identificação, avaliação e formulação de um problema; Apresentação de propostas/sugestões por todos os participantes e análise das mesmas; Pesquisa bibliográfica sobre o problema; Reformulação do problema, se necessário, apresentação de hipóteses (associada com a relevância da prevenção); Escolha dos procedimentos a aplicar; Escolha dos tipos/mecanismos de avaliação a utilizar; Implementação/ativação do projeto; Observação e avaliação dos resultados obtidos e a tomada de consciência das implicações dos mesmos. Vale ressaltar que, foram apresentados as amostras e os procedimentos utilizados para a estruturação e análise e, finalmente, os instrumentos usados.

O próximo passo será a conceituação e exposição da pesquisa, para então partirmos para o processo de recolha de dados, bem como a análise feita em cima do questionário que foi aplicado aos responsáveis pelos adolescentes. Seguimos, justificando a escolha dos participantes, os adolescentes, por serem considerados vulneráveis, e tal característica foi bastante explorada no transcorrer de toda a pesquisa aqui reportada.

Para uma melhor organização, dividimos a pesquisa em grupos, o que nos trouxe um total de 5 (cinco), e dentro destes, suas respectivas perguntas que estão relacionadas com a identificação, conectividade, caracterização, hábitos digitais e conscientização.

Em seguida, mostramos na íntegra o questionário o qual foi aplicado aos participantes, mostrando desde a orientação inicial até às perguntas que foram respondidas. E ainda, fizemos uma justificativa que ligava os quesitos do questionário às perguntas e respostas encontradas na cartilha, mostrando a importância de abordar tais conceitos.

Finalmente, mostramos como a divisão em grupos de questões foi importante para termos uma maior visão dos resultados, bem como, fazermos análises mantendo a coerência e a lógica adequada para recolher dados que serão utilizados posteriormente, isto é, apresentados e analisados. Ressaltamos a importância dessa organização estrutural de dados, pois ao fazermos a planilha conseguimos manipular os dados de maneira que estes sejam facilmente compreendidos pelo pesquisador.

CAPÍTULO 6

Proposta de um modelo que possa auxiliar os pais, os professores, o Estado e até mesmo o próprio adolescente, a reduzir os riscos cibernéticos

6.1 – Introdução

Ao longo da realização do trabalho, verificamos e aprofundamos o conhecimento relacionado com os riscos que os jovens correm ao explorarem o mundo virtual, sem o mínimo de cautela e *expertise*, tornando-os assim, alvos fáceis dos cibercriminosos.

Neste modelo de cartilha proposto tentaremos contemplar pequenas regras e cuidados os quais podem ser adotados por pais, responsáveis, professores, governo, entre outros. E como sabemos que a fase da adolescência em qualquer lugar do mundo, em regra, costuma ter comportamento semelhantes, traremos algo mais genérico para o enfrentamento do problema proposto neste trabalho.

Apesar da legislação e de alguns projetos de lei que tramitam no congresso nacional, e que se preocupam somente em punir o autor de delitos praticados por meios eletrônicos, temos que o mais importante é sempre a prevenção, e, esta, pode ser realizada com a união pessoas que podem, além de proteger os seus, divulgar e ser um multiplicador desse conhecimento preventivo.

Devemos ressaltar que a criação de leis prevendo uma punição mais severa pode inibir, em alguns casos, a prática de cibercrimes. No entanto, para que estas sejam aplicadas, as autoridades devem investir em melhores recursos para chegar até ao infrator, o qual, na maioria das vezes, permanece desconhecido.

Adicionalmente, entendemos, que protocolos de segurança e conscientização devem ser implementados com o objetivo de dificultar a ação criminosa na Internet, e, por consequência reduzir o número de jovens vítimas desses ataques virtuais.

Estudos feitos por especialistas da Polícia Federal Brasileira mostram que 80% dos ataques praticados no Brasil servem-se da técnica de engenharia social, que consiste em retirar informações sigilosas da própria vítima, utilizando posteriormente essa informação para poder

de retórica, influenciar e manipular, muitas vezes, explorando a falta de cuidados essenciais. Lembrando ainda que, os cibercriminosos são verdadeiros nômadas, no sentido de se reinventarem de acordo com as oportunidades que surgem, como exemplo, a Covid-19, que forçou muitas pessoas a usar recursos tecnológicos, seja nas suas atividades laborais ou domésticas.

6.2 – Os "modelos" existentes para prevenção de cibercrimes

Inicialmente, é importante salientar que existe preocupação por parte de alguns sites, no sentido de alertar sobre os perigos que o mau uso da Internet pode acarretar. Todavia, essas orientações são bem pontuais, pois geralmente abordam determinado tipo de ataque ou prática criminosa que é objeto de referencia como, por exemplo, as técnicas de *phishing*, ou do jogo da baleia azul.

Para chegarmos ao modelo idealizado na intenção deste trabalho precisaremos de recolher informação, também por meio de questionários, partindo da visão e do grau de conhecimento que os pais e os responsáveis possuem, quando se trata de dar liberdade aos filhos para que possam desfrutar do uso e exploração da Internet.

Ainda nesta perspetiva, temos que extrair informação relacionada com a preparação técnica de professores e educadores para avaliar da sua capacidade de enfrentar a ameaça de cibercrimes praticados contra adolescentes e sugerir planos que possam ser aplicados nas escolas, e que possam ajudar na redução dos delitos praticados por meios virtuais.

O governo por meio dos órgãos competentes e até mesmo pelo amplo acesso às mais diversas formas de mídias, possui um importante papel para a divulgação em massa de alertas, recursos e cuidados que podem ser utilizados pelos adolescentes no momento que estiverem interagindo com a gama de atividades proporcionadas pela rede mundial de computadores.

Percebemos que a mídia televisiva, especialmente, pouco ou nunca trata do tema relacionado aos cibercrimes, salvo, quando se trata de alguma edição específica sobre a matéria. Porém, é insuficiente já que não tem uma repetição e um objetivo de alcançar uma maior quantidade de telespectadores, de modo que estes realmente consigam entender e absorver as

informações necessária para a prevenção contra os cibercrimes – adicionalmente, a TV alcança com maior facilidade os pais e responsáveis que os alunos, face aos seus hábitos de consumo dos mídias.

Outro aspecto importante é que os alertas feitos pelos *sites* e outros meios de comunicação são bastante generalizadas, não sendo direcionadas ao público adolescente. O que este trabalho pretende é oferecer um conteúdo de forma específica, tendo em consideração que o público adolescente é extremamente vulnerável à atividade de cibercriminosos, o que lhes facilita o planejamento e concretização de ataques cibernéticos.

O *site safenet.org*, especializado em cibercrimes, partilha informação em formato de texto, imagens e vídeos, e ainda dados relacionados aos números de crimes praticados por meio da Internet, nas mais diversas modalidades. Disponibiliza, igualmente, pequenas cartilhas de prevenção. Estas, por sua vez, tratam de forma ampla a prevenção, dando dicas genéricas, como mostraremos também a seguir.

No primeiro momento, o *site* traz um pequeno recorte contendo informação geral relacionada com os crimes digitais, mostrando algumas e dicas e cuidados que devem ser observados para que os usuários não se tornem vítimas de cibercriminosos.

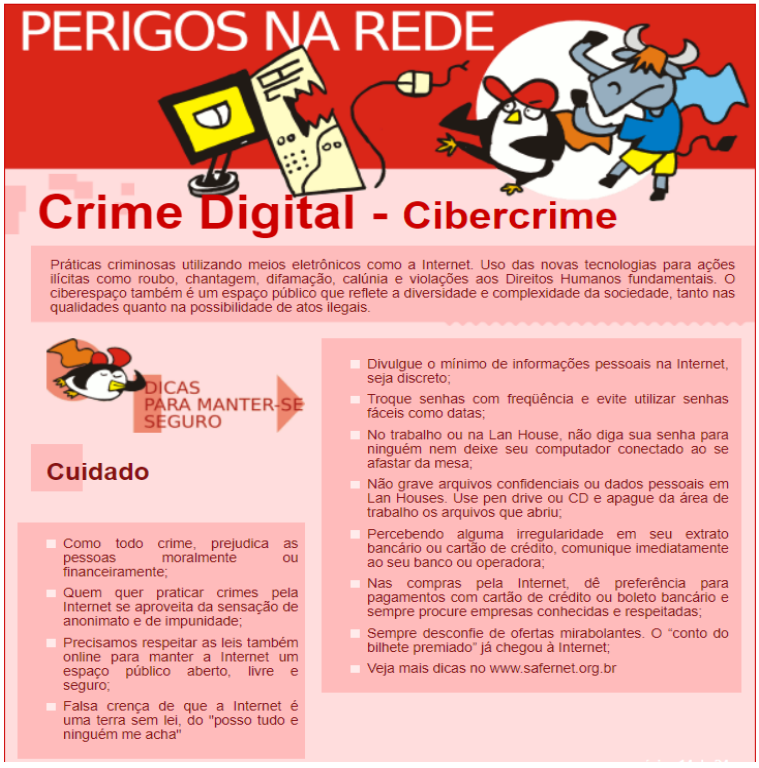


Figura 3 – Perigos na rede. Imagem extraída do site *safernet.org.br*

Os pequenos recortes trazem os delitos que estão em ênfase no momento contemporâneo, como é o caso do *ciberbullying* que já foi tratado com mais detalhe neste trabalho. Neste contexto, são mostradas as formas da prática do crime de *bullying* por meio da Internet, partilhando algumas dicas de como deve ser o comportamento do usuário diante esses ataques.

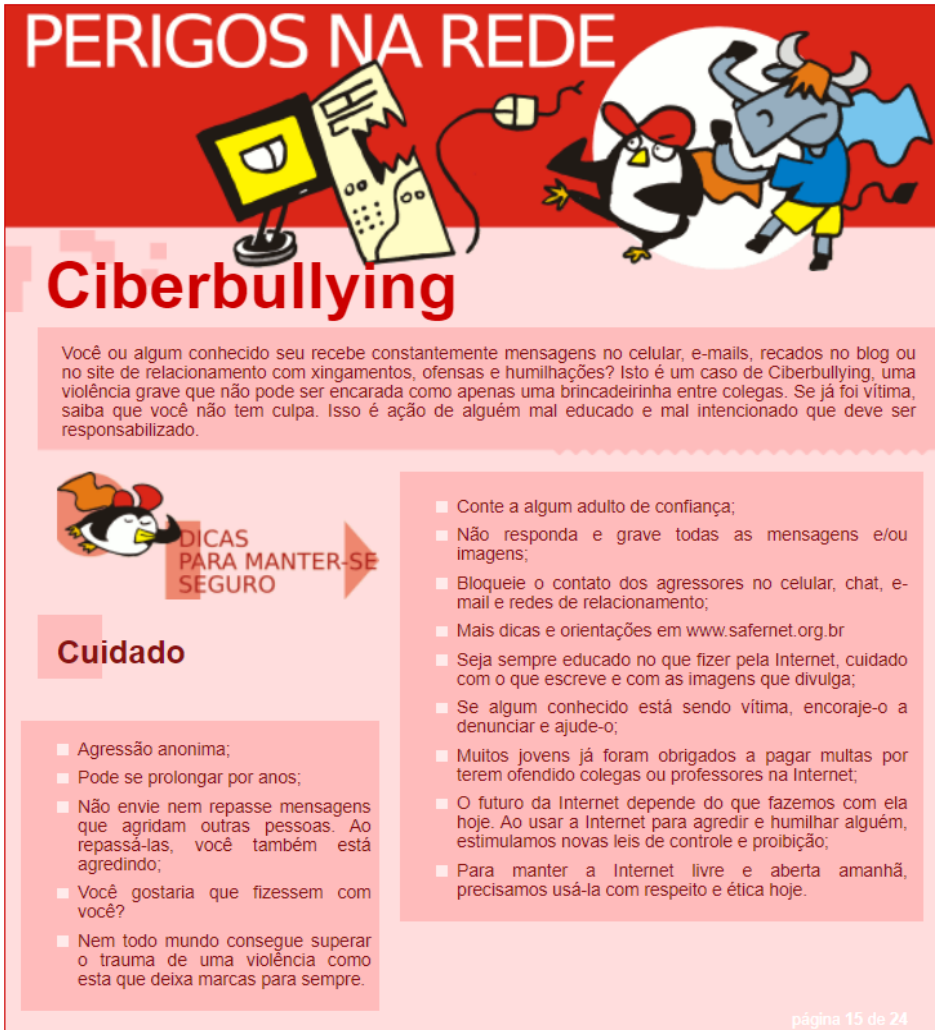


Figura 4 – *Ciberbullying*. Imagem extraída do site *safernet.org.br*

Entre os encartes existentes, é dado relevo ao que conceitua o *sexting*, o qual se tornou uma prática comum entre algumas pessoas, que por algum motivo se expõe por meio de fotos e textos sensuais. As orientações mostradas a seguir, dizem respeito ao modo geral de alertar os usuários para não serem vítimas desta situação e terem sua imagem exposta na rede mundial de computadores.

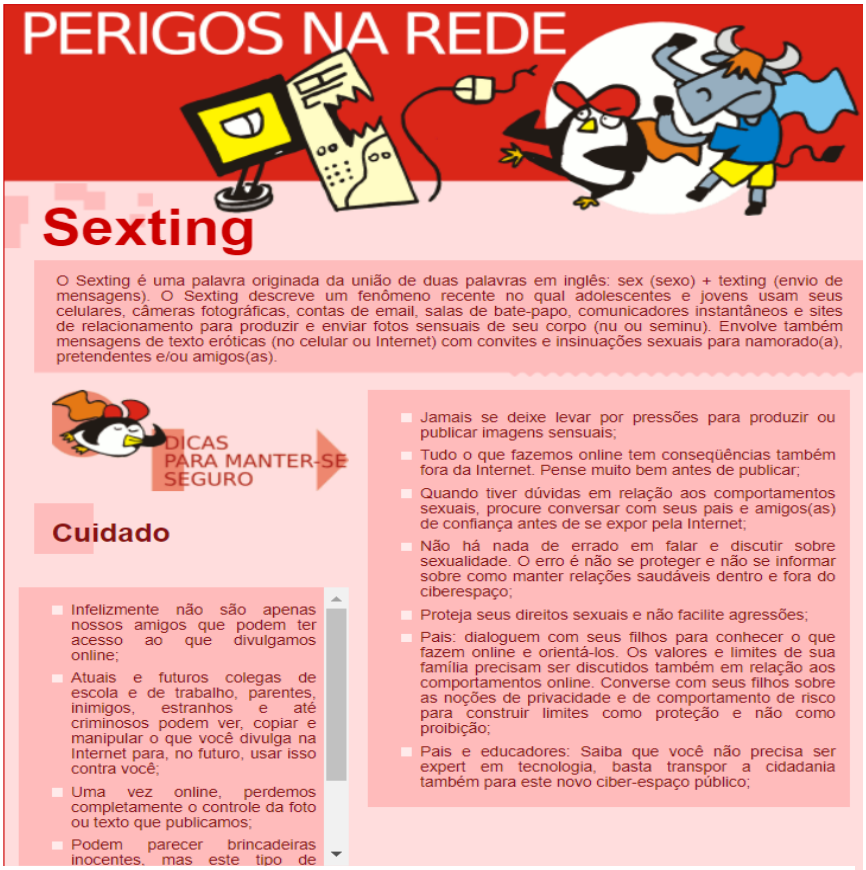


Figura 5 – *Sexting*. Imagem extraída do site *safernet.org.br*

Outro alerta feito pelo *site* é sobre o aliciamento ou chantagem *online*, que consiste no envio de imagens, recados e convites para encontros, geralmente com o objetivo de relacionamentos amorosos. Todavia, verifica-se que tais encontros podem envolver riscos como o abuso sexual e até mesmo sequestro. São igualmente realizadas algumas orientações no sentido de comunicar com as autoridades competentes.

Por outro lado, verificamos a falta de cuidado em orientar os adolescentes que gastam boa parte do seu tempo postando (publicando) fotos, textos e imagens as quais demonstram, em grande parte, os seus sentimentos. Assim, estas publicações podem ser vistas por milhares de pessoas e ainda partilhadas para outras milhares. Podem, ainda, constituir uma oportunidade para que os algozes cibernéticos planejem as estratégias perfeitas para atingir sua vítima.

Os adolescentes possuem uma necessidade de autoafirmação junto dos seus pares, fazendo com que com a exploração da sua própria imagem seja uma forma de atrair olhares dos seus amigos e consequentemente obter os mais variados tipos de elogios ou críticas. Em se tratando de fotos sensuais, estas podem ainda ser usadas para satisfazer a lascívia de pedófilos e outros tipo de pessoas com transtornos ligados ao ato sexual.

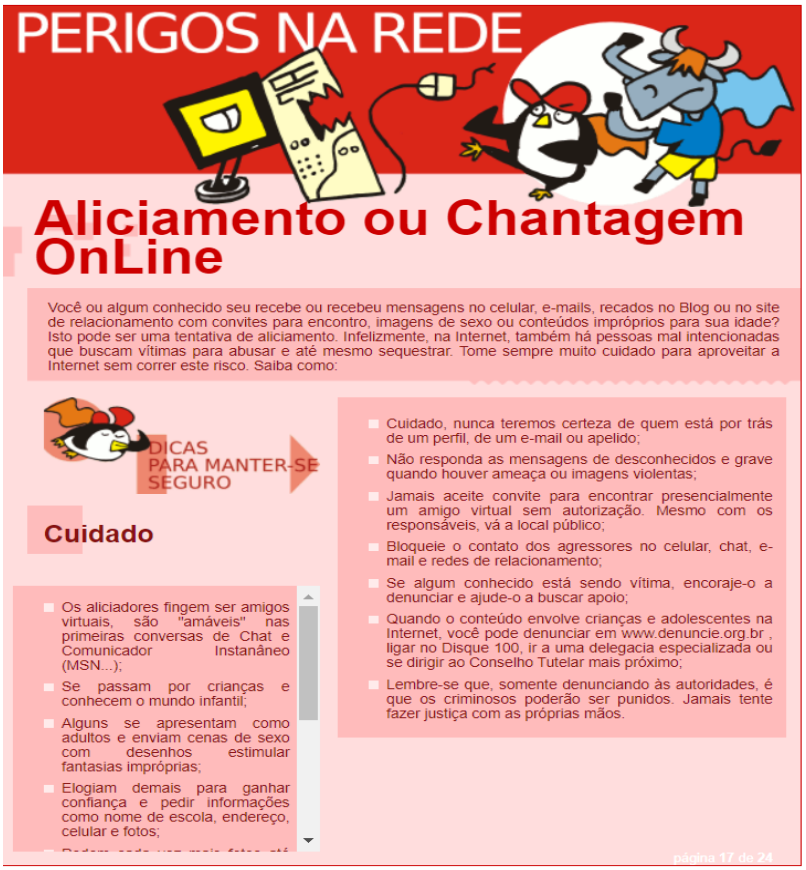


Figura 6 – Aliciamento ou chantagem *online*.
Imagem extraída do site *safernet.org*.br

Em uma sequência de infografias, são apresentados os conceitos de vírus e as dicas para se prevenir o impacto destes programas com objetivos maliciosos. É indicando os cuidados básicos para evitar que o computador seja contaminado e os dados sejam danificados ou subtraídos, por aqueles que com finalidades têm variantes, que vão do simples prazer em destruir informações constantes naquele dispositivo até à aquisição de senhas e dados capazes de gerar prejuízos de ordem financeira e moral.

Na fase pré-adulta existe uma real vontade de aquisição de bens materiais, uma das formas de conseguir aliciar um adolescente é exatamente oferecendo a esse algo que seus pais não são capazes de lhe proporcionar. Assim, ao mandar textos e fotos pornográficas, o criminoso pode utilizar de estratégias do tipo oferecimento de bens para que esses jovens venham a fazer uma espécie de troca, ou seja, permutar as suas fotos sensuais e sedutoras por objetos desejados, como roupas, sapatos, celulares (telemóveis), entre outros.

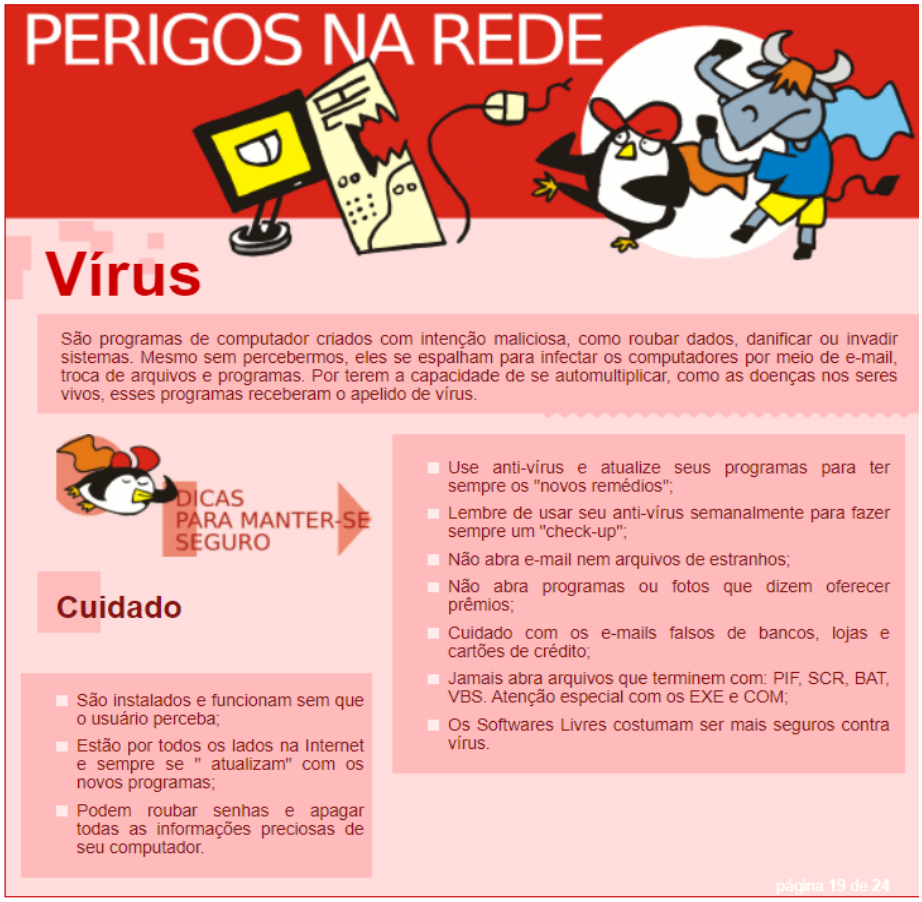


Figura 7 – Vírus. Imagem extraída do site *safernet.org.br*

Um grande número de alertas está relacionado com o roubo de dados, cuja orientação dada é no sentido de não abrir programas desconhecidos que, por exemplo, venham em anexo no correio eletrônico, a fim de evitar a invasão de privacidade. O aviso ainda indica a existência de crime na legislação vigente, todavia, não entra em detalhe e nem orienta que órgão procurar, caso ocorra tal violação.

Os prejuízos causados por vírus de computador, em geral, não atingem diretamente os adolescentes no que se refere aos delitos que estão tipificados no Estatuto da Criança e do Adolescente, já que estes têm por objetivo destruir arquivos e causar mau funcionamento no computador. Por outro lado, com a maior facilidade em seduzir os jovens, os cibercriminosos podem valer-se desses para atingir outras pessoas da família, como por exemplo, convencer um jovem a instalar determinado programa ou jogo, e estes virem acompanhados de vírus e assim causar destruição dos arquivos do computador de seus pais, os quais contém dados importantes – usando assim, os adolescentes, como vetor de ataque.

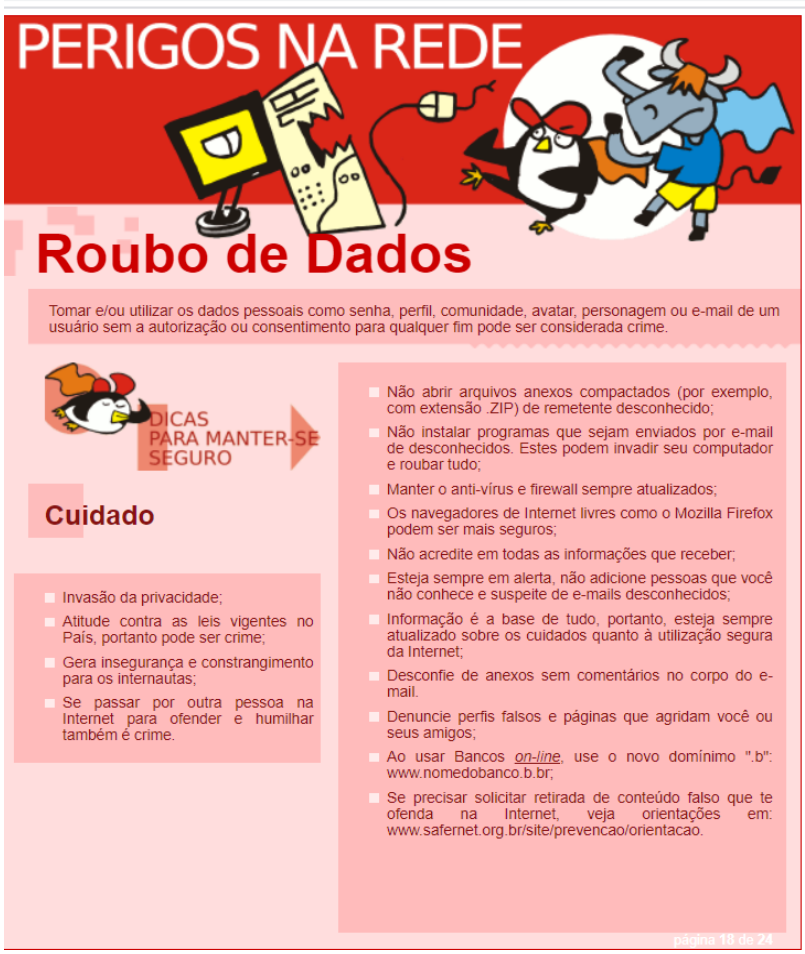


Figura 8 – Roubo de dados extraído do site *safernet.org.br*

O alerta é feito para as ações de invasão, onde as formas de prevenção mostradas são praticamente as mesmas que as expostas anteriormente, no entanto, com outras palavras. Porém, a finalidade é uma proteção geral, sem aprofundar especificamente, em nenhum usuário específico, conforme veremos.

Esta modalidade criminosa também não atinge de forma específica a atuação dos adolescentes que navegam pela internet, pois estes não possuem dados, em regra, capazes de gerar prejuízos consideráveis em caso de perda, tais como meios de pagamento ou valores associados a transações.

Por outro lado, podemos entender que estas orientações podem ser úteis, fazendo os adolescentes adquirirem como costume, a prática de cuidados para com os dados armazenados no computador, ou seja, em se tratando de jovens estas orientações ficam como precauções futuras, a menos que esses dados sejam fotos comprometedoras.

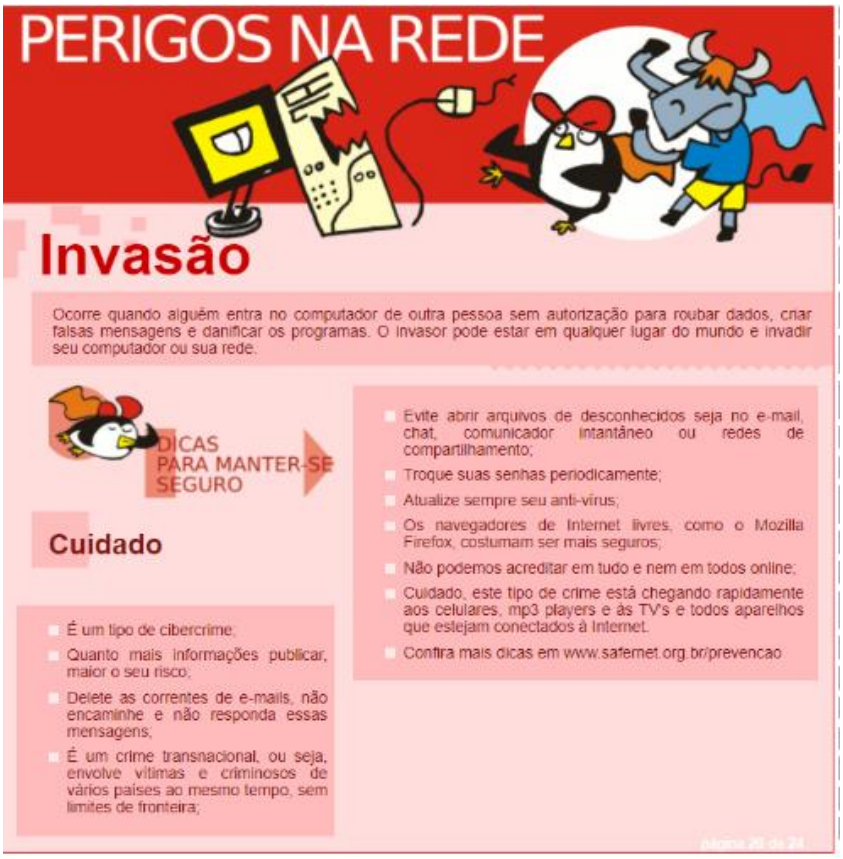


Figura 9 – Invasão extraído do site *safernet.org.br*

O *site* invoca a figura dos justiceiros virtuais e apenas orienta as pessoas que se acharam ofendidas por alguns comentários feitos em *blogues* e *sites*, para que procurem a justiça. Em alternativa a utilização de recurso *hackers*, os quais prometem invadir e apagar os comentários, bem como danificar a página que contenha os tais insultos, prejudicando assim aquela empresa ou até mesmo pessoa física que tem as suas atividades laborais realizadas por meios da Internet.

Entendemos que, este tipo de informação é de grande valia, todavia, como pode ser visto, é tratado pelo site especializado de forma bastante branda, onde deveria mostrar de facto os danos que podem ser causados por esse tipo de ataque. Em especial, os referentes ao campo psicológico, que, a bem da verdade, são os mais gravosos e podem desenvolver problemas incuráveis.

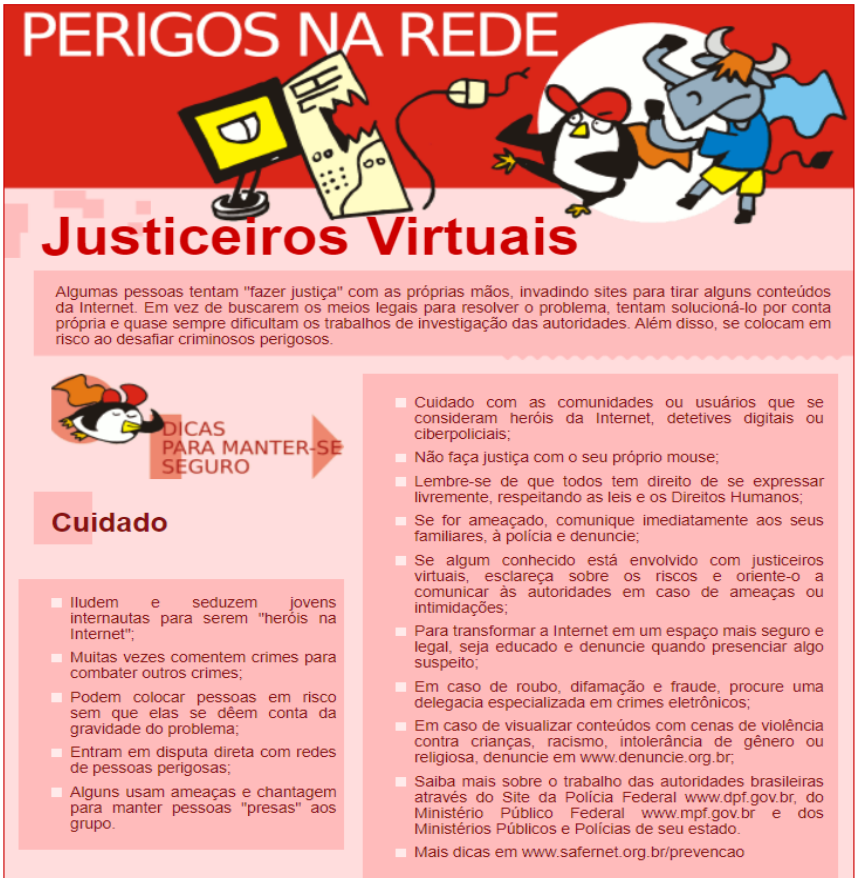


Figura 10 – Justiceiro virtual extraído do site *safernet.org.br*

Identificamos, então, uma carência significante no que diz respeito à publicação e propagação de conteúdos úteis para orientar pais, responsáveis, professores, educadores e outros, a melhor orientar os seus protegidos quando estes exploram o mundo virtual através dos diversos dispositivos que permitem a conexão com a rede mundial de computadores.

Concluímos que, não existe um modelo específico que aborde de forma, ainda que genérica, uma cartilha de instruções relacionada com as boas práticas do uso, especificamente pelos adolescentes, das tecnologias ligadas à Internet. Encontrando, somente, orientações específicas para determinados tipos de ataques, não orientadas diretamente para o público-alvo deste trabalho.

6.3 – Processo construtivo do modelo de prevenção de cibercrimes contra adolescentes

Para a construção de um modelo que tenha boa eficácia, iremos dividir por partes, mostrando os problemas jurídicos, materiais e psicológicos que podem ser objeto de ataque, bem como, as formas de prevenir cada uma dessas áreas abordadas pela cartilha que será produzida. Assim, podemos seguir uma ordem para esta construção.

- Iremos mostrar os **delitos tipificados**, principalmente, pelo Estatuto da Criança e do Adolescente no que diz respeito aos crimes praticados por meio de dispositivos conectados à Internet;
- Mostraremos os **conceitos** que estão associados diretamente com os cibercrimes, com objetivo de facilitar a identificação por parte dos usuários que vierem a ser vítima do delito ou ao menos sua tentativa;
- Colheremos **dados** para analisar o real fator de desconhecimento do assunto, visando criar uma forma eficazes de fazer este conhecimento chegar até os pais, responsáveis, professores dentre outros;
- Criaremos uma **proposta** de mostrar como o governo junto aos órgãos de segurança pública e a própria influência da mídia podem fazer para que esse conhecimento chegue a um maior número de usuários da rede mundial de computadores, tendo em vista, que estes crimes são de ordem mundial (escala global e de operação transnacional);
- **Orientar as vítimas** no sentido de procurar ajuda junto ao órgão competente, bem como fazer o procedimento correto para que o criminoso venha a ser punido pelos seus atos (no que na prática será o reporte estruturado de incidentes – um aspeto essencial para um combate informado ao cibercrime).

Na primeira etapa para a criação do modelo de prevenção, traremos ao conhecimento dos pais, responsáveis, professores etc. os crimes tipificados, especificamente, praticados por intermédio da Internet, pela legislação que protege crianças e adolescente no Brasil, tornando essa lei um ponto de apoio para toda e qualquer conduta que venha a atingir o bem jurídico protegido.

Em um segundo momento é importante mostrar os conceitos juntamente com exemplos de comportamentos que podem ser identificados facilmente como ato criminoso, fazendo com

que as vítimas possam perceber tal ação e conseguir, antes do crime se consumar, evitar a sua ocorrência e mitigar ou evitar os seus resultados.

Na terceira fase da construção desse manual de prevenção será realizada uma recolha de dados tanto para demonstrar, quanto para sermos eficientes na construção do modelo de prevenção contra cibercrimes. Ainda obteremos com esses dados, informação que nos levarão a saber qual seria uma melhor estratégia para fazer com que esse conteúdo preventivo chegue até os agentes envolvidos neste problema.

A quarta etapa consiste em demonstrar como o governo juntamente com os órgãos de segurança pública poderiam explorar o assunto, usando a mídia como aliada para que a informação chegue ao maior número de pessoas, e, principalmente, aquelas que consideramos mais vulneráveis e propícias a serem vítimas dos cibercriminosos.

Finalmente, trataremos da importante orientação que deverá ser dada para que as vítimas possam acreditar na polícia e na justiça, levando até esses órgãos informação sobre o delito sofrido pelos seus protegidos, fazendo com que providências legais sejam tomadas para que os autores venham a ser punidos na forma da lei.

Após perfazer todas as fases, a proposta é criar uma espécie de cartilha ou um guia rápido, para auxiliar na prevenção dos cibercrimes praticados contra adolescentes, de modo a levar conhecimentos mais específicos que ajudem, quem de direito, a orientar melhor os seus protegidos quando estes usam e exploram o mundo virtual por via da Internet/Web.

6.4 – Modelo proposto de prevenção contra cibercrimes

O modelo de prevenção consiste em uma pequena cartilha no formato de manual, onde teremos perguntas e respostas relacionadas com os cibercrimes e cibersegurança, para que os responsáveis legais, assim como todos os que fazem parte da formação dos adolescentes possam ser facilitadores e, assim, propagarem o conteúdo para o maior número de interessados. Tal, auxilia ao fazer da prevenção, a grande arma para redução dos cibercrimes.

Conforme visto na motivação que levou o pesquisador a escolher e estudar sobre o assunto proposto neste trabalho, foi a preocupação com os adolescentes, já que possui, inclusive, uma filha nesta fase da vida. Assim, a busca por conhecimento sobre a evolução física e mental, nos levou a perceber o quão vulneráveis são esses jovens, tendo em vista, que a formação cerebral ainda não se deu por completo e que devido ao mundo moderno ser predominantemente digital. Muitos são os que se aproveitam da fragilidade dos adolescentes, em especial, a característica de autoafirmação e de um desejo desenfreado pelo consumismo, para então arquitetar e promover seus ataques, causando danos, especialmente, emocionais, os quais podem ser irreparáveis e acarretarem problemas para toda a vida.

Devemos lembrar, sempre, que a melhor arma contra qualquer tipo de delito é a prevenção, e essa se dar, principalmente, por meio do conhecimento sobre o assunto. Não há dúvida que trazer informação sobre tema relevante e de real importância é uma reconhecida maneira de evitar o mal que pode resultar da consumação de um crime. Assim, produzir uma cartilha de prevenção, irá mitigar a possibilidade de o adolescente praticar atos que os deixe expostos aos cibercriminosos, bem como, conseguirão identificar as possíveis armadilhas feita por esses delinquentes, já que o conteúdo da cartilha mostrará o quão manipulados somos pela Internet/Web.

A seguir mostraremos um esquema de como pode ser fácil utilizar as caraterísticas dos adolescentes para os atrair, fazendo com que sejam vítimas em potencial de cibercriminosos.

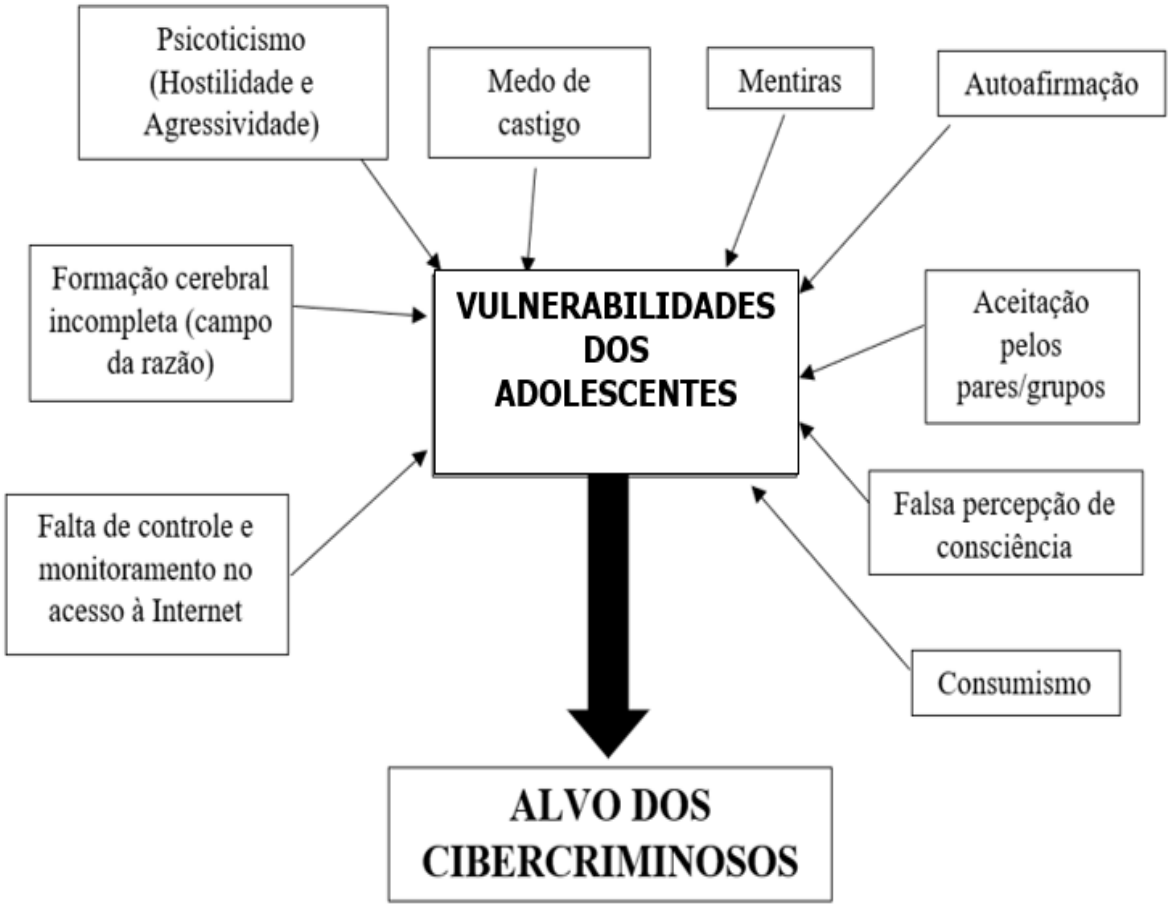


Figura 11 – Características de vulnerabilidades dos adolescentes

A produção da cartilha traz diversas questões as quais estão, diretamente, associadas com riscos, ameaças e vulnerabilidades dos adolescentes. Logo, afirmamos que uma análise minuciosa foi realizada com objetivo de identificar e fazer as devidas ligações entre essas características de vulnerabilidade que trouxemos no transcorrer do desenvolvimento da tese de doutoramento.

Vejamos no esquema a seguir.

Figura 12 – Perguntas da cartilha ligadas com riscos, ameaças e vulnerabilidades

É importante frisar que a produção de uma cartilha de prevenção, constitui uma relevante contribuição para a sociedade, tendo em consideração que a prevenção é a arma mais eficaz para todo e qualquer tipo de enfrentamento pelo qual tenhamos que passar. Esta deve ser realizada por via de um conteúdo de linguagem simples e de fácil compreensão. Assim, podemos afirmar que o conhecimento sobre o assunto e as técnicas para não deixar que o fato

ocorra, são de suma relevância, principalmente no contexto de cibercrimes e cibersegurança, onde dificilmente encontramos um material com linguagem simples de se entender, isto é, acessível para toda e qualquer pessoa, seja conhecedora ou não dos termos técnicos do mundo digital.

Finalmente, podemos trazer esse conhecimento aos pais, responsáveis e todos os que lidam com adolescentes, por meio da disponibilização da cartilha em formato PDF, o qual pode ser propagada por meio das redes sociais, e ainda podemos contar a com ajuda do governo para imprimir e distribuir nas escolas públicas, particulares, órgão governamentais e outros, fazendo, assim, com que o maior número de interessados tenha acesso e repliquem este conteúdo.

6.5 – Formas de comunicar os cibercrimes

Atualmente, existem várias maneiras de se propagar informação importante, entre elas podemos destacar:

- A Internet por meio de redes sociais, *sites* oficiais (governo, escolas, empresas, etc.). Destacamos que, esta poderá ser a maneira mais rápida para atingir mais audiência em um espaço tempo menor;
- Mídia televisiva ainda é um importante meio de propagação de conteúdo, em especial, tendo em consideração público dos pais e responsáveis pelos adolescentes;
- Palestras ministradas em órgão público, escolas etc., que contam com palestrantes que possuem conhecimento do assunto;
- Entrega de cartilhas, como esta proposta neste trabaho, com conteúdo direito e de fácil entendimento, o qual pode ser utilizado como guia para os responsáveis e professores, colocando especialmente estes últimos, como facilitadores e também disseminares para suporte e prevenção.

6.6 – A importância da universalização da cartilha de prevenção para auxiliar adolescentes sobre os cibercrimes e cibersegurança

Sabemos que os comportamentos que regem os adolescentes ao redor do mundo, em se tratando de formação biológica e psicológica, bem como no uso de tecnologias conectadas à Internet, se assemelham em muitos aspectos.

Com base nisso, acreditamos que a proposta deste trabalho, da criação de uma cartilha de prevenção para ser seguidas pelos adolescentes, pode ser universalizada, isto é, partilhadas por diversos países. Um primeiro passo é dado ao considerar a sua tradução também para a língua Inglesa, conforme partilhado no final deste relatório, em apêndice específico.

Assim, tendo em vista a internacionalização da cartilha de prevenção, a versão da cartilha no idioma inglês, contém em algumas questões, o direcionamento para procurar a informação de acordo com as regras vigentes no país que será feita a leitura.

Este partilhamento poderá ser feito pelas redes sociais, onde as pessoas podem dividir o arquivo em PDF, para que seja impresso em qualquer lugar do mundo. Assim, apesar da pesquisa ter sido realizada em um município do Brasil, poderemos contribuir de forma significativa, partilhando esta cartilha para a maior quantidade de pessoas interessadas, em especial, as que lidam ou são responsáveis legais por adolescentes.

6.7 – Cartilha de prevenção para auxiliar adolescentes sobre os cibercrimes e cibersegurança

O manual contem 30 perguntas, e as respetivas respostas, detalhadas e exemplificadas, que são dadas de forma simples e para uma fácil compreensão, visando um público que não possui conhecimento técnicos na área das tecnologias de informação.

A cartilha será montada com a seguinte sequência de questões e respectivas respostas.

Q1. **O que é a Internet?**

R1 –

Antes de falarmos do conceito de Internet, propriamente, vamos entender o que é uma rede de computadores. Quando interligamos dois ou mais dispositivos, fazendo com que eles conversem entre si, podemos chamar a tal, uma estrutura de rede (MANCILLA, 2014).

Agora que sabemos o que é rede, podemos definir a Internet como a interligação de várias redes de computadores, espalhadas pelo mundo inteiro.

Para melhor compreensão iremos ilustrar com a figura a seguir.

Figura 13 – Representação da Internet. Imagem extraída do *site* *https://www.ufpb.br/ccae/contents/imagens/internet.jpg/image_view_fullscreen*

Os dispositivos são conectados à Internet por meio de provedores de acesso, estes, por lei, devem guardar por um determinado período, informações relacionadas com o acesso dos seus clientes, o que pode ajudar a polícia a localizar e identificar possíveis cibercriminosos.

Q2. **O que é Ciberespaço?**

R2 –

É a nomenclatura dada ao ambiente virtual que é utilizado pela Internet para que o usuário possa se comunicar com outras pessoas por meios de dispositivos como o computador, o *smartphones*, etc., e assim explorar diversos meios como e-mail (correio eletrônico), *sites*, redes sociais, *e-commerce* (comércio eletrônico), *e-business* (negócio eletrônico), entre outros. É importante lembrar que este espaço possui uma dimensão imensurável fazendo com que se torne um perigo aos usuários que pretendem explorá-lo sem um conhecimento básico de cibersegurança (GONTIJO, 2007).

Figura 14 – Representação do ciberespaço. Imagem extraída do site *https://www.alfaiatedaweb.com/blogue/item/37-ciberespaco-e-a-seguranca*

A figura acima mostra o quão ilimitado é este espaço virtual. Podemos assim, ter a verdadeira dimensão, até mesmo, do quanto é difícil localizar um cibercriminoso, pois este pode estar em qualquer lugar deste planeta, e ainda temos que levar em consideração a grande quantidade de técnicas que estes podem utilizar para mascararem os seus endereços, dificultando, ainda mais, a sua real localização geográfica. A conclusão é o elevado grau de impunidade dos cibercriminosos e isto faz com que aumente a ocorrência dessa modalidade de delitos, já que é perceptível a dificuldade de encontrar o verdadeiro culpado pelo ato. Assim, podemos concluir que a prevenção ainda é a melhor maneira de se proteger desses ataques cibernéticos.

Q3. **O que é a *Surface Web, Deep Web* e *Dark Net*?**

R3 –

A *Surface Web* é a parte da Internet em que os usuários comuns acessam e se beneficiam dos mais diversos serviços como *email*, *sites* (os mais diversos), rede social, *chats*, entre outros.

Deep Web é a parte obscuras da Internet, onde os usuários comuns não conseguem entrar. Nessa área sombria trafegam informações sigilosas entre determinados grupos que querem total privacidade em suas comunicações, estes grupos podem ser montados por criminosos ou não (Pompéo, 2013).

A *Dark Net* é considerada uma parcela da *Deep Web*, essa sim, é onde os criminosos atuam praticando atos ilícitos como pornografia infantil, venda de armas, de drogas, de órgão, seitas satânicas, etc.

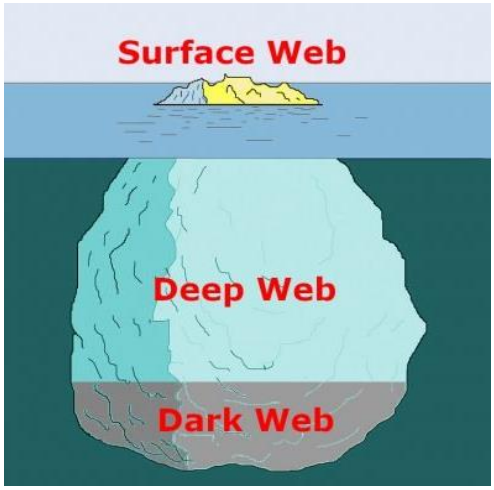


Figura 15 – Representação da Internet. Imagem extraída do site *https://tecnoblog.net/responde/como-acessar-deep-web-links/*

Estas camadas mais profundas da Internet são acessadas por programas específicos, e por óbvio, para acessar determinadas redes de comunicação, somente pessoas autorizadas pelos responsáveis pelos servidores que gerenciam esta ligação entre os computadores. Assim, verificamos a dificuldade a qual as autoridades enfrentam para conseguir se infiltrar e descobrir os delitos que circulam por esta rede sombria, ou melhor, totalmente escura. A deep web só é acessível através de permissões e inclui plataformas digitais e acesso a bancos de dados que podem e são legais, a maior parte das vezes, mas, inacessíveis para a generalidade dos utilizadores.

Q4. **O que são Cibercrimes?**

R4 –

São crimes praticados por intermédio dos dispositivos que se conectam à Internet/Web (Pinheiro, 2013), podemos trazer como exemplo:

Exemplo 01: Invadir um computador por meio de programas, e assim, subtrair ou danificar os arquivos existentes.

Exemplo 02: Utilizar uma rede social para propagar acusações falsas contra alguém.

Exemplo 03: Aproveitar conversas em salas virtuais para marcar encontros e praticar delitos como roubo, extorsão, sequestro, entre outros delitos.

Exemplo 04: Utilizar aplicativos de mensagens instantâneas (por exemplo, *WhatsApp*) para clonar contas, e praticar estelionato – fazer-se passar pelo proprietário da conta e em seguida solicitar transferência de valores ou pagamento de boletos.

Exemplo 05: Encaminhamento do usuário para *sites* falsos, idênticos aos verdadeiros, com objetivo de obter dados como a senha. E logo em seguida, entrar nas contas reais e praticar a retirada de valores ou dados importantes.

Exemplo 06: Encaminhamento de *e-mails* falsos solicitando atualização de dados em contas bancárias, ou até mesmo serviços do governo, com a finalidade de subtrair dados como cpf (identificação de cidadão), senhas, *logins*, entre outros.

Figura 16 - Ilustração de um cibercriminoso agindo. Imagem extraída do site *http://www5.tjba.jus.br/portal/cibercrimes-inscricoes-para-curso-sobre-o-tema-estao-abertas-ate-a-proxima-segunda-25/*

Q5. **O que é Cibersegurança?**

R5 –

A Cibersegurança consiste em proteger os dispositivos, principalmente os que se conectam à Internet, dos ataques maliciosos, sejam por meio de programas ou de pessoas mal intencionadas (*Hackers*, *Crackers*, entre outros).

Os programas que usuários de Internet devem ter nos seus computadores são: antivírus e antimalwares, devidamente atualizados.

Figura 17 - Ilustração de cibersegurança. Imagem extraída do site *https://promovesolucoes.com/ciberseguranca-o-que-e/*

É importante sabermos que a cibersegurança não se limita, simplesmente, aos programas específicos para proteção, os quais devem ser instalados nos nossos computadores e dispositivos. O comportamento dos usuários é o que, realmente, irá diminuir as probabilidades destes serem vítimas em potencial dos cibercriminosos (Kaspersky, 2020).

É de relevante importância que o responsável mantenha os programas de proteção sempre atualizados, para diminuir os riscos dos dispositivos, utilizados pelos seus filhos, sejam infectados por *malwares* ou vírus – incluindo os *smartphones*. Todavia, a vigilância constante é ainda mais importante, pois os ataques a adolescentes acontecem, comumente, nas redes sociais e salas de bate papo, onde os cibercriminosos usam técnicas de aproximação e buscam ganhar a confiança das vítimas, para logo em seguida, colocar o seu plano criminoso em prática. Seja este plano, o de subtrair informações importantes, seja marcando encontros para prática de atos ilícitos.

Q6. **O que é Ciberbullying?**

R6 –

Primeiramente vamos tratar do conceito de *bullying*. O termo é de origem inglesa e significa agressão e intimidação de forma reiterada. A prática de tais atos podem ser feita por intermédio da Internet, seja em uma sala de bate papo, por *email*, redes sociais, entre outros meios (Truzzi, 2019).

Esta forma de violência pode trazer lesões físicas. Todavia, alertarmos que o mais grave são as consequências psicológicas as quais podem levar o adolescente a fazer tratamentos psiquiátricos, psicológicos e muitas vezes atentar contra a sua própria vida.

Figura 18 - Ilustra uma vítima de Ciberbullying. Imagem extraída do site *https://www.istockphoto.com/br/vetor/cyber-bullying-nas-redes-sociais-e-conceito-de-abuso-online-vector-flat-desenho-gm1213369038-352617628*

Na idade compreendida como adolescência (entre os 12 e os 17 anos), o cérebro ainda não conseguiu obter a formação completa de neurônios comunicadores, isto é, a parte do cérebro que lida com a razão ainda não consegue comunicar plenamente com aquela parte responsável pelas emoções. Tal, indica o perigo de um adolescente ser bombardeado por solicitações, tendo em vista que as suas emoções estão afloradas e que estes não conseguem lidar com tais atos, na sua plenitude, de forma racional. Assim, a probabilidade do adoecimento psicológico é extremamente alta, e as consequências são desastrosas, atingindo não só as vítimas como também os seus familiares e a sociedade, a qual de alguma forma perde um membro.

Nestes casos, a busca por ajuda profissional, ou seja, um psicólogo pode ser essencial para evitar que ocorram danos irreparáveis, em especial, quando existe uma situação em que o adolescente foi vítima de um cibercrime.

Q7. **O que é Ciberstalking?**

R7 –

O termo *stalking* de origem inglesa significa perseguição. Então, o *ciberstalking* é uma perseguição por meios da Internet/Web. As vítimas passam a ser perseguidas e ter os seus passos monitorizados. Ainda pode ocorrer a utilização de fotos da vítima para criação de perfis falsos, onde esta começa a receber conteúdos pornográficos, propagandas indesejadas, entre outros, fazendo com esta começe a adoecer psicologicamente devido a este bombardeio de informações indesejadas (Truzzi, 2019).

Já existe no código penal a figura típica para combater a conduta de perseguição. Este está disposto no artigo Art. 147-A, que traz "*Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido: I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino, nos termos do § 2ºA do art. 121 deste Código; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação*".

Figura 19 – Ilustração de Ciberstalking. Imagem extraída do site *https://exame.com/pme/o-que-e-stalking-empresas/*

Ratificamos que, o cérebro de um adolescente não está preparado para lidar com críticas em massa, pois conforme já comentamos, a parte responsável pela razão ainda não se comunica bem com as demais. Assim, este age, exclusivamente, pelos sentimentos de emoções.

Q8. **O que são *Fake News*?**

R8 –

A expressão inglesa significa notícias falsas e é muito utilizado na Internet para propagar informações que não são verídicas (ou são distorcidas, contendo inverdades, suposições ou mesmo falsas alegações), fazendo com que uma grande massa populacional venha a acreditar e divulgar tal conteúdo. Muitas vezes essas falsas notícias causam pânico na sociedade (alarme social), e, geralmente, tem cunho ideológico, religioso, político ou outro com determinados fins. Essas notícias levam a população a praticarem, muita das vezes, atos impensados. Por isso, é importante sempre verificar a fonte para não se cometerem erros (Campos, 2022).

Figura 20 – Ilustração de Fake News. Imagem extraída do site *https://www.agazeta.com.br/artigos/fake-news-no-passado-eram-chamadas-simplesmente-de-mentira-0620*

Ressaltamos que essas histórias falsas, podem estar diretamente relacionadas ao delito de calúnia, em que pode ser criado um cenário falso em que se coloca determinada pessoa como sendo culpada por determinado crime, que não cometeu: por exemplo, divulgar nas redes sociais que uma pessoa praticou o crime de estupro de vulnerável contra uma criança, sendo falsa essa acusação. Na mesma ideia, temos o delito de difamação, onde pode ser propagado uma situação falsa que irá afetar diretamente a reputação da vítima perante a sociedade, por exemplo, afirmar que determinada pessoa estava em uma casa de prostituição, e assim arruinar ou afetar as suas relações/casamento.

Muito importante salientar que uma vez propagada uma informação falsa, fica muito complicado de desfazer, pois a velocidade e a dimensão que estas tomam são, muitas vezes, inimagináveis. Uma informação colocada na rede propaga-se de forma independente e não é apagada, pela sua repetição na Internet/Web, correndo em simultâneo com uma possível correção, coexistindo as duas versões.

Aconselhamos que todo e qualquer conteúdo, antes de ser publicado ou repassado e, assim, propagado pelo usuário de Internet, deve ser feita uma verificação da sua veracidade, sob pena de estar alimentando uma *Fake News*.

Q9. **O que são vírus de computadores e malwares?**

R9 –

Um vírus de computador é um programa que pode estar escondido dentro de jogos, documentos, programas (diversos) e que tem por objetivo danificar e causar mau funcionamento nos computadores ou outros dispositivos digitais. É importante que o usuário possua um programa denominado antivírus e que este esteja sempre atualizado para que possa detectar e eliminar qualquer tipo de ameaça que possa danificar ou corromper os arquivos do seu computador.

Os malwares são programas maliciosos que tem por objetivo, por regra, furtar informação e deixar o computador vulnerável para ser invadido por *Hackers*. Assim, podemos afirmar que este tipo de software são instalados no computador, com más intensões, sem a autorização do proprietário (Machado, 2017).

Figura 21 – Ilustração de vírus e malwares. Imagem extraída do *site* *https://super.abril.com.br/mundo-estranho/como-funciona-um-virus-de-computador/*

Os principais e mais conhecidos vírus, malware e técnicas maliciosas são:

- **Cavalo de Tróia ou *Trojan Horse*** – Programa que uma vez instalado no computador, o deixa vulnerável para ser invadido por criminosos cibernéticos. Este *software* poderá vir junto à instalação de um jogo ou de qualquer outro aplicativo disponibilizado gratuitamente na Internet e, após devidamente implantado no computador, tem a finalidade de capturar toda e qualquer informação digitada, desde senhas até mesmo conversas realizadas em salas de bate papo ou qualquer aplicativo que possua essa finalidade.
- ***Ransomware*** – Programa que encripta (codifica) os dados e coloca uma senha nos arquivos pessoais, e cobra um valor para possibilitar o seu desbloqueio. Aqui, o usuário pode ter um prejuízo econômico considerável. Além do tempo de inatividade associado com todo o processo de pagamento e recuperação dos dados.
- ***Spyware*** – São programas instalados no computador do usuário, sem que o mesmo perceba. Estes *software* poderá vir junto à instalação de um jogo ou de qualquer outro aplicativo disponibilizado gratuitamente na Internet e, após devidamente implantado no computador, tem a finalidade de capturar toda e qualquer informação digitada, desde senhas até mesmo conversas realizadas em salas de bate papo ou qualquer aplicativo que possua essa finalidade.
- ***Keylogger*** – Programa que tem por finalidade capturar tudo que o usuário digitar, em especial, no preenchimento de dados e senhas para entrada em aplicativos de dados sensíveis, como o caso do *homebanking*.
- ***Phishing*** – É um tipo de ataque que se utiliza da ingenuidade das pessoas que acessam à Internet, pois são utilizados mecanismos simples, fazendo com que as informações pessoais sejam repassadas pela própria vítima, pois esta está convencida que esta a preencher formulários, que aparentemente, foram solicitados por empresas sérias, como bancos ou, até mesmo, órgãos públicos.
- ***Pharming*** – Programas que direcionam o usuário para um *site* falso, todavia, este é semelhante ao *site* original, fazendo com que este digite os seus dados e senhas sigilosas e, estes sejam capturados pelos cibercriminosos.
- **Vírus de Macros** – São vírus que se escondem, geralmente, atrás de botões dos editores de textos, como o Microsoft Word ou do Microsoft Excel, e que uma vez acionado, contamina o computador, deixando este vulnerável.

- **Engenharia Social** – Técnica que utiliza o poder de convencimento para fazer com que o próprio usuário envie os dados para o criminoso, sem perceber que está sendo vítima, por exemplo: se fazer passar por funcionário do banco e dizer que precisa dos dados e senha para atualizar a conta. Em boa verdade, trata-se de aproveitar as características do ser humano, a sua curiosidade, ganância ou outro aspeto que motive a pessoa a tomar a ação pretendida e, assim, ficar cativo dos cibercriminosos, sendo manipulado para tal.
- ***Shoulder Surfing*** **(olhar por cima do ombro)** – São ações de pessoas mal intencionadas que ficam observando o usuário enquanto ele digita dados pessoais e senhas nos seus sistemas.
- ***Backdoor*** **(porta dos fundos)** – Uma vez o computador infectado por este tipo de *malware*, ele poderá ser invadido e manipulado pelo criminoso, quando for oportuno – trata-se de uma forma de controle adiada que permite posteriormente tomar posse de um computador que assim é considerado como um zombie.

Q10. **Quais programas que podem ser utilizados para proteção de alguns cibercrimes?**

R10 –

Os computadores devem ter instalados programas do tipo antivírus e antimalwares. O sistema operacional MS Windows disponibiliza a ferramenta denominada *Defender*. Todavia, existe diverso software com esta finalidade, inclusive gratuitos, que podem ser baixados e instalados. Por outro lado, temos as grandes empresas de software antivírus que cobram por essas ferramentas, mas que disponibilizam excelentes proteções. Porém, o grande segredo para se manter seguro é que estes programas estejam sempre atualizados, pois a cada dia, surgem novas variações de vírus e *malwares* (Microsoft, 2022).

Q11. **Quais os comportamentos que podem ser adotados para evitar os cibercrimes?**

R11 –

Como já observado, são diversas as formas de prática de cibercrimes. Por isso, muitos cuidados devem ser tomados para reduzir, ao máximo, a possibilidade de ser uma vítima em potencial dos cibercriminosos.

Os cuidados e comportamentos que os usuários devem ter ao acessar a Internet/Web são:

- Nunca instalar programas desconhecidos ou de fontes não oficiais;
- Nunca abrir arquivos que não saibam a origem;
- Nunca acessar *sites* de conteúdos duvidosos;
- Evitar fazer transações bancárias sem a certeza da devida segurança do *site*;
- Manter o seu sistema operacional atualizado, pois erros de segurança são constantemente corrigidos;
- Utilizar navegadores que dispõe de recursos de segurança;
- Nunca pagar boletos enviados por estranhos. Sempre confirmar o verdadeiro destinatário;
- Nunca enviar os seus dados ou senhas pela Internet (*email*, *chat*, etc.);
- Nunca envie fotos de nudez ou sensuais para ninguém, ainda que seja um seu conhecido;
- Nunca manter contato com estranhos.

Q12. **O que são comunidades virtuais?**

R12 –

É muito comum que as pessoas se interessem pelos mesmos assuntos, possuam as mesmas crenças e ideologias, pratiquem atividades iguais, etc. Assim, criam meios virtuais para trocarem informação sobre esses temas, utilizando para isso *sites*, *blogues*, redes sociais e outros, formando as comunidades virtuais. O grande perigo é que nem sempre, nessas comunidades, as pessoas de facto se interessam pelos menos temas, mas, sim, utilizam esses recursos para se aproximarem de pessoas e praticarem algum tipo de ato ilícito (Costa, 2005).

Figura 22 – Ilustração de comunidades virtuais. Imagem extraída do site *https://comunidadesvirtuaisdeaprendizagem.wordpress.com/2014/10/12/importancia-das-comunidades-virtuais-de-aprendizagem-para-a-ead/*

Q13. **O que são redes sociais? Quais os seus objetivos?**

R13 –

Redes sociais são *sites* ou aplicativos que conectam pessoas através da Internet/Web e que fazem com que estas se comuniquem e partilhem fotos, vídeos, textos, etc.

Existem vários objetivos que podemos destacar, dentre eles:

- Fazer amizades novas;
- Manter contato com amigos no mundo todo;

- Buscar relacionamentos amorosos;
- Localizar pessoas;
- Conhecer os gostos, ideologias, hobbies, etc. das pessoas que lhe interessam;
- Buscar emprego e trabalho;
- Buscar conhecimento acadêmico;
- Oferecer serviços e produtos;
- Fazer protestos contra algo ou alguém;
- Divulgar livros, artigos, projetos, ações sociais, etc;
- Fazer campanha política, solidária, educacional, etc.;
- Divulgar trabalhos;
- Aumentar visibilidade da atividade laboral desenvolvida;
- Buscar parcerias para negócios.

Figura 23 – Ilustração de redes sociais. Imagem extraída do site *https://cakeerp.com/blog/redes-sociais/*

Q14. **Qual a faixa etária que a lei considera adolescente?**

R14 –

Conforme o Estatuto da Criança e do Adolescente a faixa etária para ser considerado adolescente é de 12 anos completos até 17 anos – isto é, ter menos de 18 anos de idade (Brasil, 1990).

Figura 24 – Ilustração da Lei de Crianças e Adolescentes. Imagem extraída do site *https://www.novacandelaria.rs.gov.br/site/noticias/administracao/15967-13-de-julho---dia-do-eca-%E2%80%93-estatuto-da-crianca-e-do-adolescente*

Q15. **O que é uma pessoa vulnerável? Porque um adolescente é considerado vulnerável aos cibercrimes?**

R15 –

Pessoas vulneráveis são aquelas mais propensas a serem vítima de determinadas ações, como roubos, furtos, estelionatos, estupros e outros. Em se tratando de cibercrimes, podemos afirmar que os adolescentes possuem uma certa vulnerabilidade, pelo facto de estarem passando por uma fase de descobertas, onde a autoafirmação e o desejo de tomar decisões são consideravelmente relevantes, e ainda tem a questão de não temerem pelas consequências as quais possam ter, caso se utilize de forma desenfreada o acesso à Internet/Web.

Podemos ainda ressaltar que, o consumismo nessa fase é bastante elevado, e o desejo de possuir determinados objetos, roupas, etc. pode ser um fator que facilita o cibercriminoso de se

aproximar da sua vítima, e este contato ocorre na maioria das vezes pelas redes sociais, onde adolescentes demostram os seus gostos e desejos.

Figura 25 – Ilustração de vulnerabilidade dos adolescentes. Imagem extraída do site *https://pt.dreamstime.com/adolescentes-deprimidos-lan%C3%A7am-conflito-ciberbuloso-com-depress%C3%A3o-dos-pais-amor-sem-resposta-problemas-de-puberdade-adolescente-image194711688*

Temos duas partes do cérebro, entre várias outras: a que lida com sentimentos e com a razão. Os adolescentes ainda não formaram 100% desta parte responsável pela razão, motivo pelo qual não conseguem ter uma visão lógica de determinada atitude, e isso é um fator primordial para que estes sejam alvos de cibercriminosos.

Q16. **Porque o adolescente é manipulado, facilmente, de forma psicológica?**

R16 –

Os adolescentes ainda não estão com os neurônios de comunicação totalmente finalizados, isto é, os transmissores que fazem com que a informação passe pelo campo da razão, dentro do cérebro, ainda não foram totalmente formados. Assim, tal processo, faz com que este haja mais pela emoção do que pela razão.

Lembrando que os adolescentes buscam a autoafirmação, para que possam ser aceites pelos seus pares. Por este motivo, estes podem ser ludibriados e manipulados por um cibercriminoso que detenha este conhecimento e uma capacidade de explorar este fator e manipular os adolescentes. Pois, este irá atingir um ponto fraco da psique da vítima, fazendo com ela pense que está agindo corretamente e de acordo com os padrões das comunidades das quais fazem parte e às quais querem pertencer.

Figura 26 – Ilustração de manipulação. Imagem extraída do site *https://pensarbemviverbem.com.br/6-tipos-sutis-de-manipulacao-psicologica/*

Essa manipulação pode levar o adolescente a praticar condutas ilícitas, bem como ações que irão afetar drasticamente o seu estado psicológico, podendo deixá-lo dependente de medicações psicotrópica ou até levá-lo ao cometimento de suicídio.

Q17. **Quais as estratégias utilizadas para atrair os adolescentes?**

R17 –

A técnica utilizada para atrair os adolescentes, fazendo com que estes sejam vítimas em potencial, é demonstrando comportamentos e gostos semelhantes, isto é, participando de grupos que despertam o seu interesse, sejam os que tratam de músicas, ideologias políticas, estilos de vestuário, estética, entre outros assuntos que norteiam esta fase de transformação que é a adolescência e constituem os seus interesses.

Após, os cibercriminosos, terem o primeiro contato com as suas possíveis vítimas, estes procuram conhecer ainda mais o comportamento delas e tendem a fazê-las pensar que encontraram um amigo ou um par perfeito que, pensam exatamente da mesma maneira e possuem os mesmos gostos. Consequentemente, começam a confiar e passam a ser manipulados, o que pode acarretar uma série de problemas, inclusive psicológicos.

Figura 27 – Ilustração de como os adolescentes são atraídos. Imagem extraída do site *https://www.showmetech.com.br/quais-sao-as-tendencias-entre-os-jovens-da-geracao-z-em-2019-segundo-pesquisa/*

A adolescência é uma fase marcada pelos sonhos de consumo, isto é uma caraterística explorada pelos cibercriminosos, tendo em vista que estes oferecem, justamente, os produtos que os jovens têm interesse em possuir. Assim, facilmente os adolescentes são atraídos e logo estão sendo, parcial ou totalmente, manipulados por estes delinquentes. Ressaltamos que, os meios virtuais podem ser apenas uma ferramenta para a prática de crimes presenciais, isto é, o criminoso utiliza os recursos da tecnologia para se aproximar da vítima e praticar as mais diversas modalidades criminosas.

Q18. **O que o Estatuto da Criança e do Adolescente traz sobre crimes praticados pela Internet?**

R18 –

De forma bem direta e simples iremos apresentar os delitos trazidos pelo E.C.A. e que estão diretamente ligados com a Internet, os quais devem ser reconhecidos pelos responsáveis, caso ocorra a prática de uma dessas ações que mencionaremos a seguir (Brasil, 1990).

Delito 1 – Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente.

Delito 2 – Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Delito 3 – Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Delito 4 – Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Delito 5 – Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual.

Delito 6 – Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

Você sabe o que significa o termo "Cena de sexo explícito ou pornográfico?

Para efeito dos crimes previstos nesta Lei, a expressão "*cena de sexo explícito ou pornográfica*" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

IMPORTANTE

Vários são os delitos, praticados contra os adolescentes, que estão no código penal e que podem ser aplicados se praticados por meio da Internet, por exemplo, ameaça, constrangimento ilegal, difamação, injúria, perseguição dentre outros.

Figura 28 – Ilustração de uma vítima de crime cibernético. Imagem *extraída do site https://www.centrosermais.com/cyberbullying-o-que-precisa-saber/*

Q19. **O adolescente pode praticar atos criminosos pela Internet?**

R19 –

O Estatuto da Criança e do Adolescente estabelece que o adolescente não pratica crime e sim ato infracional, já que as punições são diferentes das aplicadas aos adultos. Ressaltamos, porém, que existem penalidades que podem trazer como consequência, a privação da liberdade para aplicação de medidas socioeducativas (ECA, 1990).

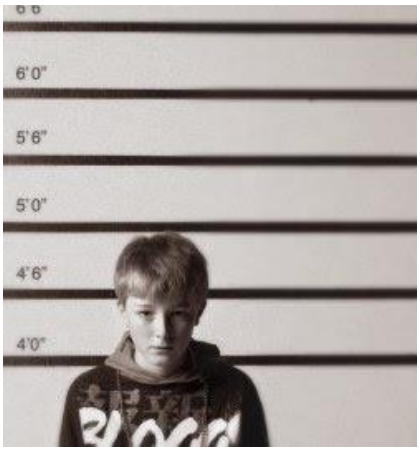


Figura 29 – Ilustração de um adolescente sendo punido pelo ato infracional. Imagem extraída do site *https://veja.abril.com.br/coluna/cacador-de-mitos/mito-os-adolescentes-cometem-menos-de-1-dos-homicidios-do-brasil-e-sao-36-das-vitimas/*

Q20. **Qual seria o tempo ideal de acesso para um adolescente?**

R20 –

Não existe um tempo ideal para o acesso à Internet, pois devemos analisar alguns fatores, como:

- Tempo de pesquisas (entre 1 e 2 horas);
- Tempo para entretenimento (entre 1 e 2 horas);
- Tempo para trabalho (em média 8 horas – com intervalos curtos de descanso – o que daria o total de 6 horas e 30 minutos em frente da tela do computador).

Podemos afirmar que, a cada 50 minutos em frente a tela, devemos parar ao menos 10 minutos, os quais, podemos utilizar para fazer pequenas refeições, beber água, lavar o rosto, fazer necessidades fisiológicas, enfim, tirar a mente daquele foco.

Figura 30 - Ilustração do excesso de tempo de acesso à Internet.
Imagem extraída do site
https://paranoiasnfm.wordpress.com/2012/01/14/vicio-internet-alcool-drogas/

Q21. **Quais os males que podem trazer o excesso de horas conectados à Internet?**

R21 –

Muitos são os prejuízos que um acesso desenfreado pode trazer, tanto para saúde física como a psicológica. Podemos citar alguns desses males:

- Problemas na visão, pois a intensa entrada de feixes de luzes, sem intervalo e por grandes períodos diários, pode causar danos no globo ocular;
- Alimentação pode ficar comprometida, uma vez que os adolescentes ficam horas a fio concentrados e com olhar fixo na tela do computador ou *smartphone*, e esquecem de se alimentar. Tais atitudes podem ser danosas para diversos órgãos, em especial, o estômago;
- Problemas nos nervos da mão, que podem trazer consequência como a LER (Lesão por Esforço Repetitivo) a qual é considerada uma síndrome constituída por um grupo de doenças – tendinite, tenossinovite, bursite, epicondilite, síndrome do túnel do carpo, dedo em gatilho, síndrome do desfiladeiro torácico, síndrome do pronador redondo, mialgias –, que afeta músculos, nervos e tendões dos membros superiores principalmente, e que sobrecarrega o sistema musculoesquelético. Esse distúrbio provoca dor e inflamação e pode alterar a capacidade funcional da região comprometida;
- A forte incidência da luz da tela do computador pode causar insônia, uma vez que o cérebro fica ativado no momento que era para estar repousando;
- Dores nos ombros, pescoço e coluna, devido ao usuário ficar na mesma posição por horas;
- A perda de memória pode ocorrer, principalmente, em casos dos usuários que são viciados em jogos, pois estes tendem a se concentrar demasiadamente e acaba por deixar de alimentar o cérebro com outras informações;
- O efeito *google* afeta o cérebro humano de tal forma que passa a armazenar o mínimo de informações, já que estar condicionado a buscar tudo com facilidade nesta ferramenta de pesquisa – afetando também a memória e a capacidade de memorizar e em consequencia, o entendimento e a aprendizagem;
- A nomofobia é o medo de não ter a tecnologia presente a todo momento, isto é, o usuário fica totalmente dependente de dispositivos que se conectam à Internet, como exemplo,

temos o uso de *smartphones*, os quais se tornaram uma ferramenta inseparável das pessoas;

- A síndrome do toque fantasma onde o cérebro estar tão ligado ao telefone celular (telemóvel) que o usuário sente vibrações e ouve toques sem que o esteja emitindo tais sinais. Isto pode levar a comportamento compulsivos e crise de ansiedade;
- E, por último, o FOMO (*fear of missing out*) consiste no medo de perder alguma coisa, isto é, tem a necessidade de saber o que as outras pessoas estão a fazer, gerando assim, crises de ansiedade.

Figura 31 – Ilustração dos problemas de saúde que podem causar pelo excesso de horas na Internet. Imagem extraída do site *https://www.tecmundo.com.br/internet/6449-jovens-podem-ter-problemas-de-saude-se-expostos-a-mais-de-tres-horas-na-internet.htm*

Q22. **O que são os desafios da Internet e quais seus objetivos?**

R22 –

Muitos são os desafios que surgem e se espalham pela Internet: perigosas práticas que põem em risco a saúde ou mesmo a vida dos participantes ou de terceiros (Pelarigo, 2021). São exemplos:

Baleia Azul ou *Blue Whale* – Este desafio tem o objetivo de fazer o participante praticar atos que diminuam o seu medo da morte, e por fim, é mesmo realizado um incentivo ao suicídio;

Alfabeto do diabo – Faz com que os adolescentes se mutilem, usando objetos pontiagudos para desenhar letras chinesas nas mãos, sob pena de serem amaldiçoados;

Desafio do desodorante – Os participantes devem inalar a substância em aerossol e manter a boca fechada pelo máximo de tempo. Este desafio pode levar a paragem cardíaca, devido às substâncias que compõe esses produtos;

Desafio da água fria – Tem por objetivo despejar um balde de gelo sobre a cabeça, o que traz um risco de hipotermia;

Sal e gelo – Faz com que os participantes coloquem sal e gelo nas mãos e mantenham fechadas o máximo de tempo possível. Como consequência, o participante pode ter graves queimaduras.

Jogo do fogo – O participante despeja um produto inflamável no corpo e acende o fogo e sai correndo para se jogar em uma piscina, lago, etc. O risco aqui é notório, uma grave queimadura pode ocorrer;

Jogo da Momo – Uma boneca manipuladora, pelo criminoso, que faz vídeos para crianças e adolescentes, pedindo para fazer alguns desafios macabros que podem levar a morte.

Figura 32 - Ilustração dos desafios da Internet. Imagem extraída do *site* *https://www.curiosidades.com.br/2019/04/desafios-mais-perigosos-da-internet/*

Q23. **Quais os males que as redes sociais podem trazer?**

R23 –

Os adolescentes, geralmente, utilizam redes sociais para se comunicar com seus pares, e essa forma de interagir requer demonstrações de atitudes que são admiradas por estes.

A postagem de fotos em determinados lugares, com determinadas roupas, com determinadas pessoas influentes, tudo isso são postados, e o adolescente espera ansiosamente as curtidas (gostos). O problema é quando vem as críticas, o *ciberbullying* e outras atitudes que

mexem com o psicológico destes, promovendo ou despoletando crises de ansiedade, síndrome do pânico ou depressão, podendo mesmo ter consequências drásticas como o suicídio.

Os adolescentes não estão preparados para receberem qualquer tipo de crítica em massa ou em público e as redes sociais são especialistas neste tipo de ação, expondo todos a situações extremas. Uma vez que a foto ou publicação cai na rede social, em questões de minutos, já vira noticiário para o mundo inteiro, e por conseguinte vem um bombardeio de comentários, os quais muitas vezes são desagradáveis e mexem profundamente com estes que estão em fase de amadurecimento e não sabem lidar com certas situações que a vida nos impõe – mesmo para adultos, estas situações podem ser extremas, quanto mais para adolescentes.

Figura 33 - Ilustração dos males das redes sociais. Imagem extraída do site *https://www.vittude.com/blog/impactos-redes-sociais-saude-mental/*

Ressaltamos ainda que, a exposição feita em redes sociais podem facilitar a prática de delitos, já que mostram a rotina das pessoas como, a escola que estuda, o restaurante que frequenta, os bens que possuem, o local onde moram, as condições financeiras, o rol de amizades, ou seja, expõe, literalmente, todas as informações necessárias para um criminoso planejar um ataque e avaliar o potencial das suas vítimas.

Q24. **O que são nudes? O que é *sextorsion*?**

R24 –

O termo nudes vem da língua inglesa e significa nus. Hoje é muito comum jovens tirarem fotos que exibem partes íntimas dos seus corpos e depois enviarem a pessoas de seu relacionamento ou até mesmo para estranhos, confiando que estes não irão propagar as imagens. É aí que entra o *sextorsion* (extorsão sexual) que é uma extorsão, isto é, o criminoso exige dinheiro da vítima para não espalhar pela Internet as suas fotos íntimas. A consequência disso é que muitos adolescentes chegam a praticar o suicídio devido à vergonha que sentem por tal comportamento e por não darem conta dos milhares de insultos que são feitos. Por vezes, em vez de dinheiro, é realizada chantagem para o cibercriminoso obrigar o adolescente a realizar certo tipo de ações, entre as quais, pratica de atos de natureza sexual, em troca da não divulgação das imagens.

Figura 34 – Ilustração de sextorsion. Imagem extraída do site *https://prezi.com/p/rrpzqm_40iio/grooming-sexting-sextorsion/*

Ressaltamos que, jamais, devem ser enviadas fotos ou vídeos de cunho sensual ou sexual, mesmo que seja para pessoas para as quais se acredite serem de confiança. Pois, ainda que estas pessoas não propagem as imagens, pode ocorrer a perda do dispositivo, o que fará com que o conteúdo armazenado possa ser acessado por um estranho, e aqui podemos ter dois caminhos: se utilizar esse conteúdo privado para extorquir o proprietário, ou divulgar nas Internet pelo simples prazer, o que, tanto um quanto o outro, trará prejuízos que podem ser irreparáveis (Safernet, 2022).

Q25. **Quais os principais delitos que podem passar do campo virtual para o real?**

R25 –

Muitos cibercriminosos utilizam da Internet apenas como ferramentas para praticarem os delitos no mundo real (Código Penal, 1940). Os delitos mais comuns são:

- **Roubo**: Após conhecer as condições financeiras da vítima, marca encontros amigáveis para então subtrair os pertences, utilizando violência ou ameaça grave;
- **Furto**: Conhecendo a rotina da vítima, o criminoso pode planejar entrar na sua residência e subtrair os seus pertences;
- **Latrocínio**: Com o objetivo de obter valores ou bens de valores consideráveis, o criminoso, que tem conhecimento da fortuna da vítima, planeja o ataque tirando a vida desta para atingir os seus objetivos;
- **Estelionato (Burla)**: Marca encontros com a vítima e faz com que esta acredite nas suas histórias fantasiosas, induzindo-a a lhe entregar valores ou pertences;
- **Estupro**: O estuprador, geralmente, escolhe determinados perfis de pessoas para praticarem os seus ataques, e estes podem ser, facilmente, encontrados nas redes sociais. Por exemplo, após se aproximar e ganhar a confiança da vítima e até mesmo da família, praticam o crime de estupro;
- **Estupro de vulneráveis**: Com as mesmas técnicas utilizadas para a prática de estupro, os criminosos também o fazem para violentar menores de 14 anos, os quais são considerados vulneráveis perante o código penal brasileiro;
- **Extorsão mediante sequestro**: Ao conhecer as posses da vítima, bem como a sua rotina, o criminoso planeja o sequestro com objetivo de obter valores como forma de resgate.
- **Homicídio**: O criminoso que tem a intenção de matar a vítima, se faz passar por terceiro, marca um encontro amigável, e assim, atrai a vítima para então tirar a sua vida.

Figura 35 – Ilustração de delitos iniciados na Internet e consumado no cenário real.
Imagem extraída do site *https://masterjuris.com.br/principais-crimes-contra-o-patrimonio/*

Q26. **Como atuam os cibercriminosos?**

R26 –

Existem diversos tipos de cibercriminosos, e o seu modo de agir e objetivos são bastantes específicos. Mostraremos as nomenclaturas dadas aos cibercriminosos e o que eles geralmente atacam e como agem (Machado, 2017):

- **Cibercriminoso**: São pessoas que utilizam a Internet para praticarem os mais diversos tipos de delitos, como: estelionato, extorsão, furto, difamação, etc.
- ***Lammer***: São pessoas que não possuem nenhum conhecimento, como um *Hacker*, mas, que utilizam ferramentas prontas para fazer seus ataques;
- ***Hackers***: São pessoas com conhecimento avançado que testam esses conhecimentos para modificar software e hardware, de modo a conseguir os seus objetivos;
- ***Crackers***: São invasores, ou seja, criminosos de verdade, que utilizam os seus conhecimentos para prejudicar um sistema ou pessoas;
- ***Phreaker***: É o especialista em invasão de sistemas telefônicos;
- ***Carder***: É o especialista em fraudes com cartões de créditos;
- ***War Driver***: É o especialista em redes *wireless* que aproveita a vulnerabilidade das redes para as invadir, atuando em especial, nas redes wireless públicas;
- ***Defacers***: São pessoas que invadem *sites* e modificam o *layout*, deixando a sua marca registrada, como uma espécie de pichação, como objetivo que mostrar a sua façanha para os demais cibercriminosos;
- ***Script Kiddies***: São pessoas inexperientes e que procuram alvos fáceis para aplicarem os seus poucos conhecimentos, e assim obterem algum lucro;
- **Guru**: São pessoas com altíssimo nível de conhecimento, podemos dizer que são os pais dos hackers.

Figura 36 – Ilustração que mostra diferença entre *Hackers* e *Crackers*.
Imagem extraída do *site https://brainly.com.br/tarefa/12242173*

Q27. **O que é o capitalismo de vigilância virtual?**

R27 –

O termo capitalismo de vigilância foi criado para enfatizar que, na atualidade, os dados possuem um valor económico bastante significativo e que podem ser vendidos e realizar dinheiro com eles. A Internet monitora e compila todos os dados dos usuários, para saber os seus interesses e assim fomentar a indústria de bens de consumo.

Não é à toa que quando o usuário pesquisa determinado produto, este começa a surgir, em forma de propaganda, no *email*, anúncios dentro de outros *sites* e até telefonemas lhe oferecendo o produto pesquisado. Tudo isso, não é por acaso, podemos afirmar que tudo que se faz pela Internet é captado e processado, e que essas informações são valiosas para muitos interessados (Nippes & Guidolini, 2020).

Figura 37 - Ilustração do capitalismo de vigilância. Imagem extraída do site *https://www.newslinereport.com/negocios/nota/capitalismo-de-la-vigilancia-la-regulacion-a-monopolios-tecnologicos-*

Q28. **Quais as consequências psicológicas que podem ter, as vítimas de cibercrimes?**

R28 –

É de grande importância tratar sobre o aspecto psicológico daqueles que são vítimas de cibercrimes. Estes adolescentes podem ser fortemente afetados. Vale a pena ressaltar que, o psicológico sendo afetado, torna muito provável que algum órgão do nosso corpo venha a se manifestar negativamente, transformando a situação em doença física.

Algumas doenças psicológicas podem afetar gravemente uma vítima de cibercrimes, dentre elas (Minha Vida, 2022):

- **Ansiedade** – É uma doença que atinge o psicológico a ponto de fazer com que a mente tenha preocupações excessivas ou constantes de que algo negativo vai acontecer. Essas crises de ansiedade podem trazer, também, doenças físicas. Exemplo: alguém que fica esperando ansiosamente as pessoas comentarem as suas postagens nas redes sociais;
- **Depressão** – É um transtorno psicológico que faz com que a pessoa afetada fique triste e não tenha mais vontade de realizar tarefas que, anteriormente, eram prazerosas. Exemplo: se iludir com as postagens feitas por pessoas na Internet, e que podem causar uma sensação de que todos são felizes e bem-sucedidos, menos você;
- **Síndrome do Pânico** – São crises de ansiedade repentinas e intensas com forte sensação de medo e mal-estar, acompanhada de sintomas físicos. Exemplo: *Fake News* mostrando estatísticas falsas sobre doenças, o que faz com que você se sinta amedrontado com a possibilidade de ser atingido pela enfermidade e venha a morrer;
- **Síndrome do Pensamento Acelerado** – É um sintoma associado à ansiedade o qual, devido a uma grande quantidade de informação processada diariamente, faz com que a mente fique agitada, hiperpensante, impaciente e que podem levar à depressão, síndrome do pânico, estresse, entre outras patologias. Exemplo: pessoas que passam o dia sendo bombardeadas por informações vindas de *e-mails*, *WhatsApp*, *Instagram*, *Facebook*, *sites*, entre outras platadormas digitais ou serviços;
- **Nomofobia**: É o medo irracional de ficar sem o seu telefone celular (telemóvel) ou ser incapaz de usar o telefone por algum motivo, como a ausência de um sinal, ou por ter sido vítima de um vírus o qual fez o celular parar de funcionar, ou pelo término do pacote de dados ou o término de carga da bateria. Exemplo: pessoas que se tornaram dependentes de telefone celular pois, todas as suas informações e atividades são realizadas por meio deste aparelho.

Q29. **Qual delegacia de polícia especializada procurar em caso de cibercrimes?**

R29 –

Dentro da estrutura de delegacias de Polícia Civil, temos uma especializada denominada Divisão de Prevenção e Repressão de Crimes Tecnológicos (DPRCT). Esta tem por finalidade identificar e localizar os cibercriminosos. Podendo, em seguida, entregar informação ao poder judiciário para que este seja objeto de penalização conforme a legislação criminal vigente no país.

Q30. **Quais os problemas sociais que podem acarretar a não comunicação dos cibercrimes?**

R30 –

Quando uma vítima ou seu representante legal deixa de informar o delito para as autoridades policiais competentes, fortalece-se o fenômeno denominado Cifra Escura, a qual consiste no desconhecimento, por parte das autoridades, dos crimes cometidos. Ressaltamos ainda que, tal conduta pode alimentar a prática de cibercrimes, uma vez que os cibercriminosos saem impunes, e, assim, vitimizando cada vez mais os membros da sociedade.

6.8 – Como saber mais sobre tema (sites sugeridos)

Existem uma quantidade sigmificativa de informação disponível, da qual se destacam os seguintes sites:

- *https://www.avast.com/pt-br/c-category-security* (Informação sobre cibersegurança);
- *https://www.policiacivil.pa.gov.br/* (Site oficial da Polícia Civil do Estado do Pará);
- *https://new.safernet.org.br/* (Informação sobre crimes cibernéticos, comportamentos na web, segurança digital, etc.);
- *http://www.planalto.gov.br/ccivil_03/leis/l8069.htm* (Lei que prevê Estatuto da Criança e do Adolescente);
- *http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm* (Código Penal Brasileiro);
- *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm* (Lei do Marco Civil da Internet);
- *http://segup.pa.gov.br/* (Site da Secretaria de Segurança Público do Estado do Pará);
- *https://www.kaspersky.com.br/resource-center/definitions* (Definições relacionadas a cibersegurança);

6.9 – Resumo do capítulo

Percebemos e observamos ao longo dos estudos para realização da proposta que, muitos *sites* mostram as notícias relacionadas com cibercrimes, e algumas vezes trazem, rápido e de forma genérica, alertas relacionados com a forma de proteção contra aquele tipo específico de ataque.

Os *sites* especializados em conteúdos envolvendo cibercrimes e cibersegurança, por sua vez, mostram de forma geral os principais tipos de ataques realizados por intermédio da Internet/Web, juntamente com algumas dicas para que o usuário possa se prevenir, reduzindo, assim, a possibilidade de ser vítima.

A grande carência de informação sobre estes assuntos, diz respeito à vulnerabilidade, em especial, de adolescentes como vítimas dos delitos praticados na Internet/Web. Existe uma necessidade de um conteúdo simples e de ampla divulgação para que todos os envolvidos nesta "guerra virtual" possam ter ferramentas para auxiliar a combater os males dos quais este grupo etário mais vulnerável e, que estão em fase de transformação psicológica, possam vir a se prevenir para não serem vítimas em potencial.

A nossa proposta é produzir uma espécie de cartilha de orientação que possa além de explicar os delitos, trazer mecanismos que ajudem a proteger os adolescentes, bem como mostrar o amparo jurídico que estes podem ter e como agir em caso de serem vítimas de cibercrimes.

O principal objetivo é trazer um notório e importante contributo para os envolvidos neste tão importante tema, que são: pais, responsáveis legais, educadores, professores, governo, o próprio adolescente e todos os que se interessem em combater esse mal tão presente na vida dos usuários de Internet.

Partido da ideia de que o comportamento dos adolescentes ao acessarem a Internet, são semelhantes no mundo inteiro, foi realizada uma versão em inglês da cartilha de prevenção para auxiliar adolescentes sobre os cibercrimes e cibersegurança. Assim, conseguimos atingir uma maior população, fazendo com que o contributo deste trabalho tenha ainda um maior alcance.

Com base na proposta tratada anteriormente, foram consideradas 30 perguntas e as suas respectivas respostas, com o objetivo de esclarecer os principais conceitos trazidos pela Internet, bem como um conteúdo básico sobre cibercrimes e cibersegurança, voltados com mais especificidade para os adolescentes. Vale ressaltar que, há ilustrações através de imagens que representam o assunto exposto, fazendo assim com que haja uma melhor compreensão sobre a temática explorada, em especial, dirigidas ao público da cartilha: os pais ou responsáveis pelos adolescentes, professores e os próprios adolescentes.

Complementamos com uma lista de URLs que podem ser acessadas para obter conhecimento atualizado sobre cibersegurança. Incluímos, também, os endereços eletrônicos das instituições oficiais ligadas à segurança pública do Estado do Pará, bem como a legislação que rege os delitos relacionados no contexto do Brasil.

Finalmente, verificamos que há a necessidade de mostrar um conteúdo simples e principalmente que tenha uma grande escala de divulgação por meio da mídia, fazendo assim com que a informação e orientação chegue ao maior número de potenciais vítimas, pois, a relevância do tema é de âmbito mundial.

CAPÍTULO 7

Resultados da aplicação oficial do questionário

7.1 – Introdução

A importância da aplicação dos questionários, seja de forma *online* ou impresso, consiste na recolha de dados e na confirmação de informaçao relevante para o estudo realizado no âmbito deste trabalho, bem como, para a aplicação da proposta a qual a tese se alicerça.

Os dados serão agrupados em uma planilha do Microsoft Excel e, trabalhados, com uso de fórmulas, para extração de informação relevante para uma análise da proposta da cartilha sobre cibersegurança, já descrita.

Este capítulo apresenta os resultados da aplicação do questionário a pais ou responsáveis sobre cibersegurança de adolescentes, na cidade de Belém do Pará no Brasil. O questionário foi proposto com o objetivo de extrair informação relacionada com o conhecimento dos responsáveis em relação aos assuntos de cibercrimes e cibersegurança, bem como, obter algumas características importantes dos adolescentes e dos seus responsáveis. O instrumento encontra-se organizado em 21 (vinte e um) questões, estruturadas em 5 (cinco) grupos, a saber: Identificação; Conectividade; Caracterização; Hábitos digitais; e Consciência.

O questionário foi aplicado no período de 25 de março à 03 de abril, de 2022, por vias eletrônicas e fisicamente impresso, com recurso próprio, tanto no uso de plataforma *Google Forms*, quanto em papel por impressão dos questionários. Do processo resultaram a aplicação de 200 questionários válidos, cujos resultados são apresentados a seguir.

7.2 – Apresentação dos resultados

Antes do participante começar a responder às 21 (vinte e um) perguntas contidas no questionário, feito na plataforma *Google Forms*, ele deveria aceitar participar de tal pesquisa científica, por via de um consentimento informado, explicitamente, e que foi realizado com o seguinte texto:

> *Por favor, leia atentamente as informações para os participantes: Entendo que minha participação e voluntária e que posso desistir de continuar respondendo às perguntas, desde que seja antes de enviar a resposta e que meus dados serão utilizados com finalidade de estudos científicos e nada mais. Eu aceito que os dados coletados serão publicados em sites, artigos e apresentados na defesa da tese. Eu aceito participar desse estudo científico.*

Importante ressaltar que, foram impressos vários questionários e solicitado que os participantes preenchessem manualmente, de modo a contemplar também situações em que as competências tecnológicas de pais e responsáveis eram menores ou inexistentes.

7.2.1 – Grupo 1 – Grupo Identificação (Adolescente)

A pergunta de número 1 (um) contida no questionário foi: Que idade tem o adolescente? A qual deveria ser respondida por meio de número inteiro que podia variar entre 12 e 17 anos, já que está é a faixa etária dos adolescentes de acordo com o Estatuto da Criança e do Adolescente, legislação vigente no Brasil.

Extraímos deste primeiro questionamento que, o valor mínimo apresentado foi de 12, e o máximo de 17, os quais representam a faixa de idade do público-alvo da pesquisa. Ainda podemos retirar a média de idade que é de 14,4 anos. A idade que mais aparece, ou seja, a moda, é de 12 anos, isto é, a idade mínima considerada. Vale ressaltar que, a mediana que é de 14 anos, significando que o grupo é mais próximo do limite inferior da idade considerada para adolescente.

A quantidade adolescente com 12 anos foi de 41, com 13 anos, 29, com 14 anos, 37, com 15 anos, 30, com 16 anos, 27, e com 17 anos, 36. Falando em percentagem, teríamos a representação de 20,5% com idade de 12 anos, 14,5% com 13 anos, 18,5% com 14 anos, 15% com 15 anos, 13,5% com 16 anos e 18% com 17 anos.

A tabela e o gráfico a seguir mostram o número e a idade dos adolescentes cujo responsável participou do preenchimento do questionário.

12 anos	13 anos	14 anos	15 anos	16 anos	17 anos
41	29	37	30	27	36

Tabela 4 – Idades dos adolescentes resultantes da aplicação do questionário

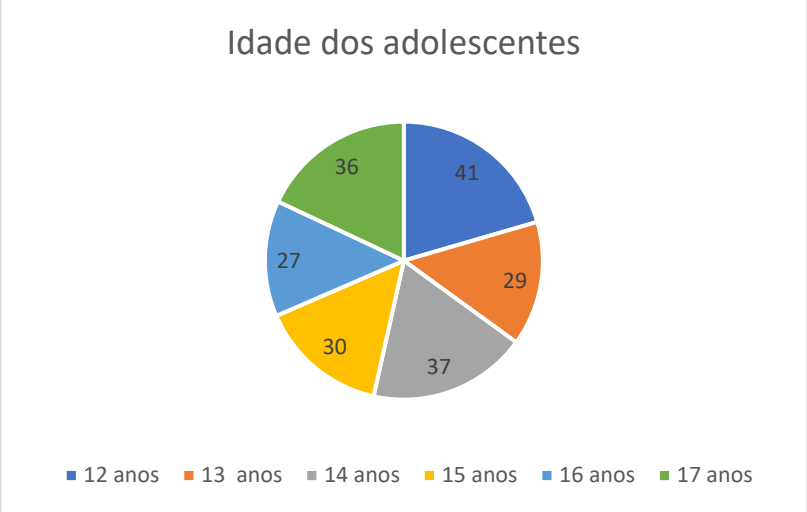


Gráfico 1 – Idades dos adolescentes resultantes da aplicação do questionário

A segunda pergunta encontrada no questionário é: Qual o gênero do adolescente? Esta deveria ser respondido com texto trazendo as opções masculino ou feminino.

Obtivemos que o número de adolescentes masculinos é de 86 e feminino é de 114. Assim, podemos extrair que, a pesquisa contemplou um universo maior de adolescentes do sexo feminino. Em percentagem isso seria representado por 43% do sexo masculino e 57% feminino.

A tabela e o gráfico a seguir mostram o número de participantes que possuem filhos do sexo masculino e feminino.

Masculino	86
Feminino	114

Tabela 5 – Número de adolescentes do sexo masculino e feminino

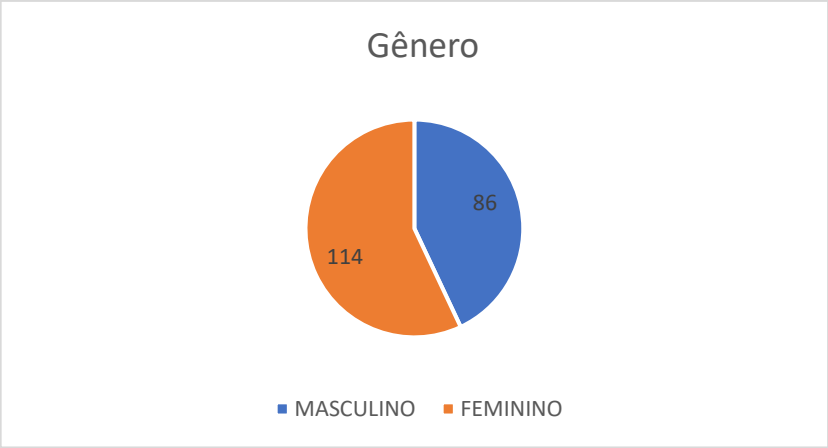


Gráfico 2 – Número de adolescentes do sexo masculino e feminino

O questionamento de número 3 (três) traz o seguinte: Que ano/curso frequenta o adolescente? As opções, tendo como parâmetro a regra de escolaridade dos adolescentes, foram de 1º grau, 2º grau ou Curso Profissionalizante. Como resposta obtivemos 126 adolescentes que frequentam o 1º grau, 70 o 2º grau e 4 cursos profissionalizante. Verificamos a maior incidência em alunos no primeiro grau, já que o quantitativo somado de adolescentes de 12, 13 e 14 anos é de 107, e esta idade, como regra, cursa o ensino fundamental, isto é, o 1º grau. Em percentagem isso seria representado por 62,5% cursam o 1º grau, 35,5% o 2º grau e 2% curso profissionalizante.

A tabela e o gráfico a seguir mostram a escolaridade dos adolescentes.

1º grau	126
2º grau	70
Curso Profissionalizante	4

Tabela 6 – Escolaridade dos adolescentes

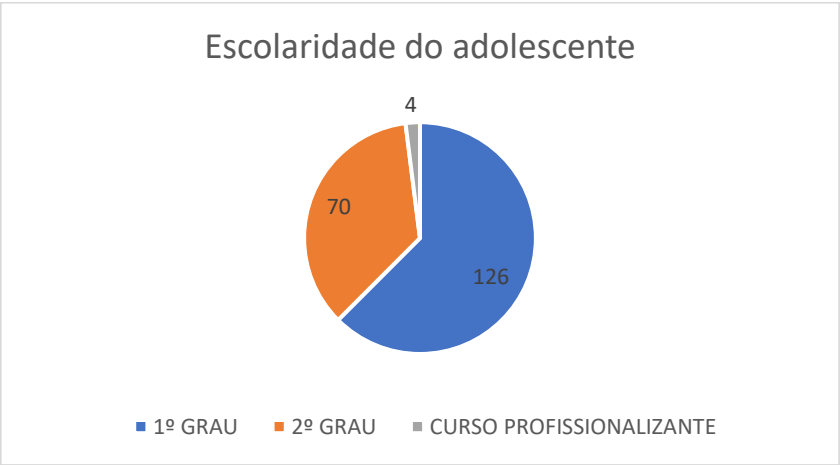


Gráfico 3 – Escolaridade dos adolescentes

7.2.2 – Grupo 2 – Grupo Conectividade (Adolescente)

A pergunta de número 4 (quatro) traz o seguinte questionamento: O adolescente possui acesso à dispositivos conectados à Internet (*smartphone*, *tablet*, computador etc.)? Onde o participante respondeu sim ou não, apenas, já que não nos preocupamos em saber qual o dispositivo o adolescente usava para se conectar à Internet.

O resultado foi de unanime, isto é, os 200 adolescentes possuem dispositivos conectados à rede mundial de computadores. Isso nos leva a concluir que, a conectividade no mundo moderno está cada vez maior, em especial, entre os jovens. Em percentagem isso seria representado por 100% sim e 0% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que possuem dispositivos conectados à Internet.

Possui dispositivos conectados à Internet	200
Não possui dispositivos conectados à Internet	0

Tabela 7 – Conexão com a Internet

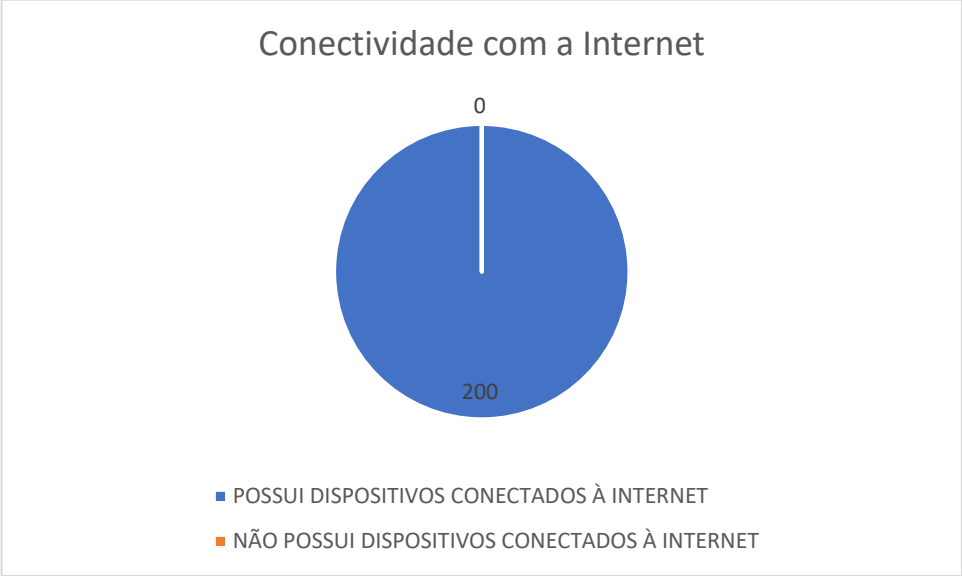


Gráfico 4 – Conexão com a Internet

O quinto questionamento traz a seguinte pergunta: O adolescente possui alguma rede social (*Facebook*, *Instagram*, *WhatsApp*, etc.)? O entrevistado respondeu sim ou não, apenas, não tivemos a preocupação de saber, especificamente, qual rede social o adolescente utiliza.

Obtivemos os valores de 189 que disseram que seus filhos tinham rede social e 11 disseram que não. Podemos perceber que a maioria dos jovens fazem parte de alguma dessas redes. Em percentagem isso seria representado por 94,5% sim e 5,5% não.

A tabela e o gráfico a seguir mostram o número de adolescente que possuem algum tipo de rede social.

Possui rede social	189
Não possui rede social	11

Tabela 8 – Adolescentes que possuem rede social

Gráfico 5 – Adolescentes que possuem rede social

A pergunta de número 6 (seis) é: O adolescente possui acesso às suas contas em rede social? O participante da entrevista deveria responder sim ou não. Esse questionamento é bastante interessante na medida que o adolescente pode não possuir rede social, no entanto, pode se valer das redes sociais de seus responsáveis para, inclusive, entrar em locais liberados apenas para maiores de idade.

O resultado que obtivemos foi que 128 adolescentes tem acesso a redes sociais dos pais e 72 não. Em percentagem isso seria representado por 64% sim e 36% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que possuem acesso a conta de rede social do responsável legal.

Tem acesso as redes sociais do responsável	128
Não tem acesso as redes sociais do responsável	72

Tabela 9 – Acesso a rede social dos pais ou responsáveis legais

Gráfico 6 – Acesso a rede social dos pais ou responsáveis legais.

7.2.3 – Grupo 3 – Caracterização (Responsável)

Temos no questionamento de número 7 (sete) o seguinte: O responsável está ligado ou tem acesso às publicações nas redes sociais do adolescente? Isso irá mostrar o quantos os pais podem não ter a consciência dos riscos iminentes do filho ter um acesso desregrado e livre. Outra vez, os participantes tinham a opção de resposta de sim ou não.

Extraímos o resultado de que, 160 diz que conhece as postagens do seu filho e, 40 não sabem que publicações o adolescente faz. Em percentagem isso seria representado por 80% sim e 20% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que possuem ou não conhecimento das postagens dos adolescentes.

Tem conhecimento das publicações do adolescente	160
Não tem conhecimento das publicações do adolescente	40

Tabela 10 – Conhecimento das publicações

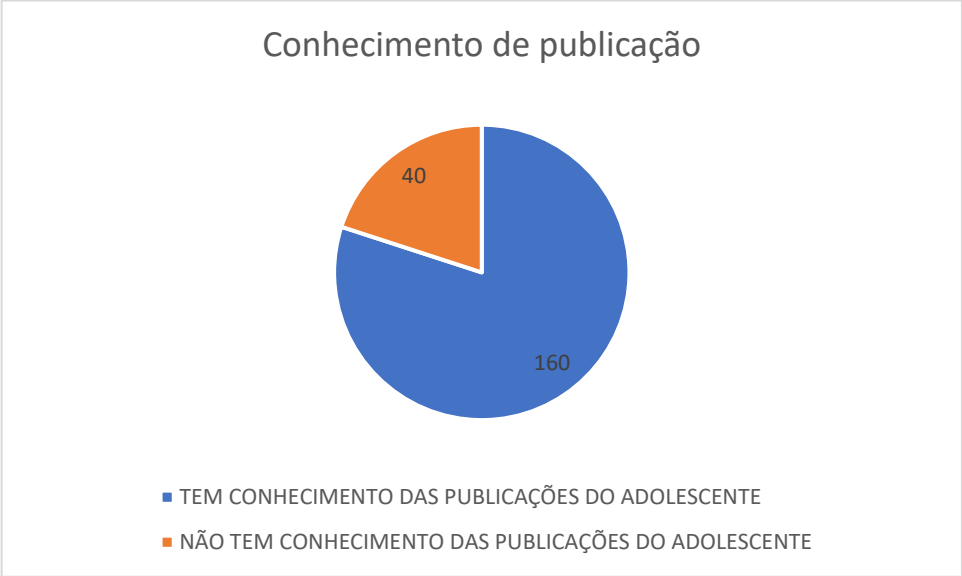


Gráfico 7- Conhecimento das publicações.

A oitava pergunta foi: Qual a escolaridade do responsável? Aqui nos preocupamos em saber a escolaridade do responsável, para posteriormente analisar e verificar se tem alguma ligação entre tal informação e os demais questionamentos.

Verificamos que 31 responsáveis possuem o 1º grau (ensino fundamental), 74 o 2º grau (ensino médio) e 95 o nível superior. Em percentagem isso seria representado por 15,5% cursam o 1 grau, 37% o 2º grau e 47,5% o superior.

A tabela e o gráfico a seguir mostram o número do nível de escolaridade dos participantes da entrevista, isto é, a quantidade que possuem 1º grau, 2º grau ou nível superior.

1º grau	31
2º grau	74
Superior	95

Tabela 11 – Escolaridades dos pais ou responsáveis legais.

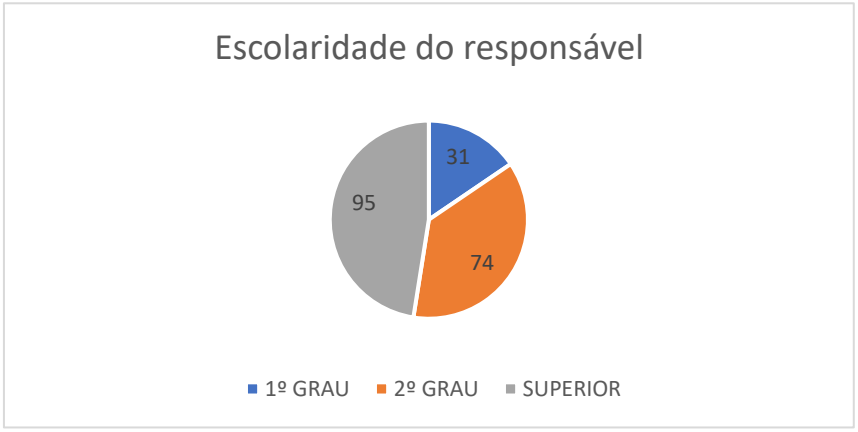


Gráfico 8 – Escolaridades dos pais ou responsáveis legais.

O questionamento número 9 (nove) traz a seguinte indagação: O responsável faz o controle desse acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal? A resposta a ser dada era, simplesmente, sim ou não. Isso demonstrará o quão desprotegido pode estar o adolescente ao explorar o ciberespaço sem um monitoramento adequado e essencial.

Os números obtidos foram de 142 que, disseram que monitoram o acesso do filho de alguma forma, e 58 não fazem nenhum tipo de monitoramento. Em percentagem isso seria representado por 71% sim e 29% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que fazem ou não o monitoramento do acesso do adolescente.

Responsáveis monitora/controla o acesso do adolescente	142
Responsáveis não monitora/controla o acesso do adolescente	58

Tabela 12 – Controle/monitoramento de acesso à Internet

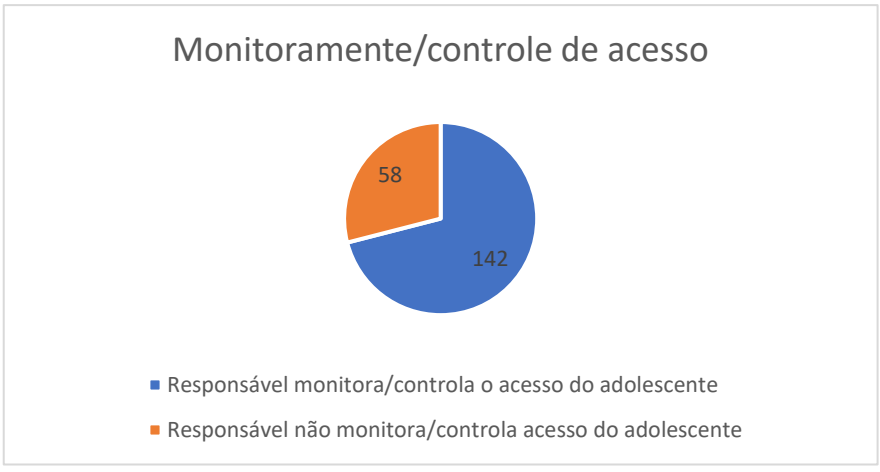


Gráfico 9 – Controle/monitoramento de acesso à Internet

Na pergunta de número 10 (dez) trazemos o seguinte questionamento: O responsável conhece todos os contatos virtuais do adolescente? Os participantes tinham a opção de resposta de sim ou não. Vale ressaltar, a importância do questionamento, já que saber com quem os filhos se relacionam virtualmente, é um conhecimento o qual pode servir de alerta e até mesmo de possível intervenção por parte do responsável.

Foi recolhido o número de 73 responsáveis que dizem conhecer todos os contatos do filho e 127 que não conhecem. Em percentagem isso seria representado por 36,5% sim e 63,5% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que dizem conhecer ou não os contatos virtuais do adolescente.

Responsável conhece todos os contatos do adolescente	73
Responsável não conhece todos os contatos do adolescente	127

Tabela 13 – Conhecimento dos contatos virtuais dos adolescentes

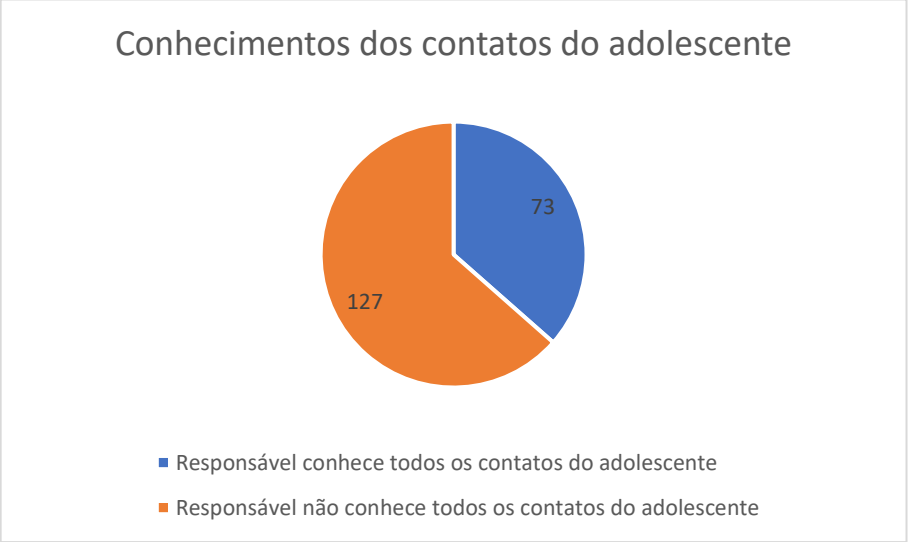


Gráfico 10 – Conhecimento dos contatos virtuais dos adolescentes

7.2.4 – Grupo 4 – Hábitos digitais (Adolescente)

A oitava pergunta do questionário vem trazendo a seguinte indagação: Quanto tempo em média o adolescente fica conectado à Internet? Neste quesito a resposta foi dada por meio de números inteiros que podiam variar de 1 até 24 horas, tendo em vista, o acesso diário.

Os números obtidos foram: 10 acessam por 1 hora por dia, 25 por 2 horas, 23 por 3 horas, 31 por 4 horas, 25 por 5 horas, 23 por 6 horas, 5 por 7 horas, 16 por 8 horas, 01 por 9 horas, 14 por 10 horas, 01 por 11 horas, 22 por 12 horas, 01 por 13 horas, 01 por 14 horas, 01 por 15 horas, 0 por 16 horas, 0 por 17 horas, 01 por 18 horas (máximo composto na resposta). Em percentagem isso seria representado por 5% por 01 hora, 12,5% por 2 horas, 11,5% por 3 horas, 15,5 por 4 horas, 12,5% por 5 horas, 11,5% por 6 horas, 2,5% por 7 horas, 8% por 8 horas, 0,5% por 9 horas, 7% por 10 horas, 0,5% por 11 horas, 11% por 12 horas, 0,5% por 13 horas, 0,5% por 14 horas, 0,5% por 15 horas, 0% por 16 horas, 0% por 17 horas e 0,5% por 18 horas.

A tabela e o gráfico a seguir mostram o número de horas que os adolescentes passam conectados à Internet.

1 hora de acesso	10
2 horas de acesso	25
3 horas de acesso	23
4 horas de acesso	31
5 horas de acesso	25
6 horas de acesso	23
7 horas de acesso	5
8 horas de acesso	16
9 horas de acesso	1
10 horas de acesso	14
11 horas de acesso	1
12 horas de acesso	22
13 horas de acesso	1
14 horas de acesso	1
15 horas de acesso	1
16 horas de acesso	0
17 horas de acesso	0
18 horas de acesso	1

Tabela 14 – Horas conectados à Internet

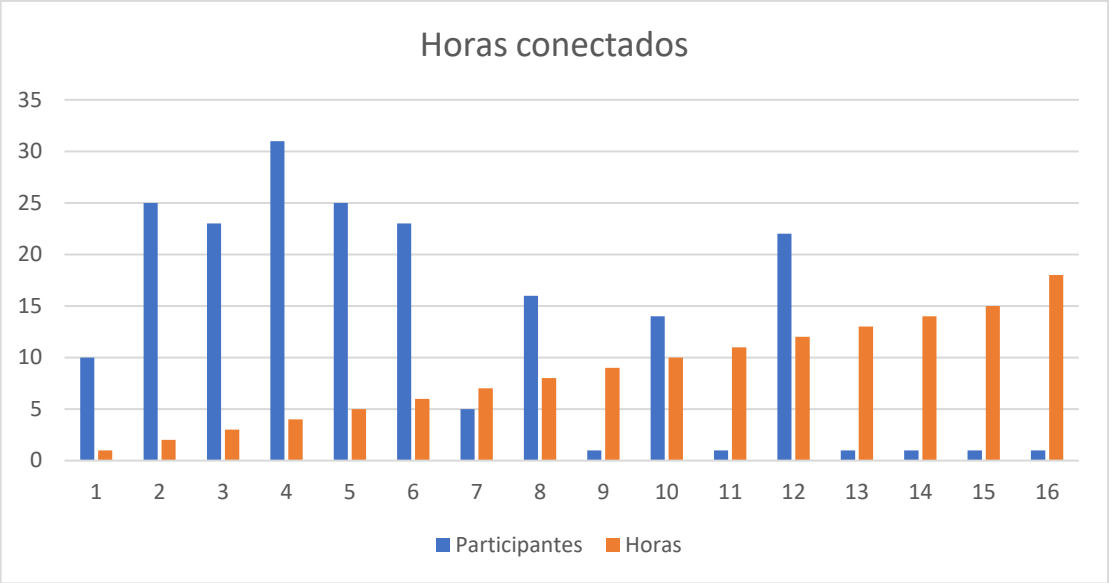


Gráfico 11 – Horas conectados à Internet

O questionamento de número 12 (doze) traz: O adolescente possui atividades extraescolares ou desporto, de forma frequente? Bastava responde sim ou não, sem a necessidade de especificar a atividade praticada.

O número de adolescente que praticam atividades extraescolares é de 149, e de 51 que não possuem essa prática. Em percentagem isso seria representado por 74,5% sim e 25,5% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que possuem atividades extraescolares.

Possui atividade extraescolar	149
Não possui atividade extraescolar	51

Tabela 15 – Atividade extraescolar

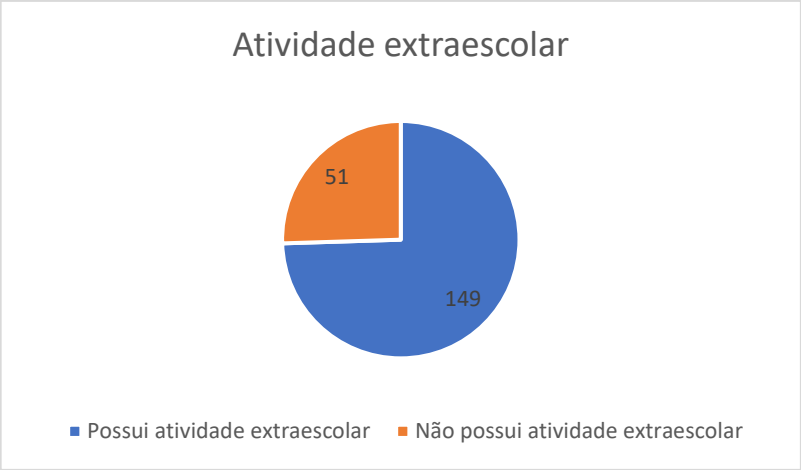


Gráfico 12 – Atividade extraescolar

A pergunta de número 13 (treze) é: O adolescente possui um grupo de amigos regulares com quem se encontra fisicamente? A resposta a ser dada é sim ou não. Este quesito é importante para saber o quão os adolescentes estão perdendo este contato físico com outras pessoas de seu ciclo de amizade.

O número de adolescente que se encontram fisicamente com os amigos é de 152, enquanto 48 não participam dessa interação física. Em percentagem isso seria representado por 76% sim e 24% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que possuem grupos de amigos e com eles costumam se encontrar fisicamente.

Costumam se encontrar, fisicamente, com amigos	152
Não costumam se encontrar, fisicamente, com amigos	48

Tabela 16 – Encontros físicos

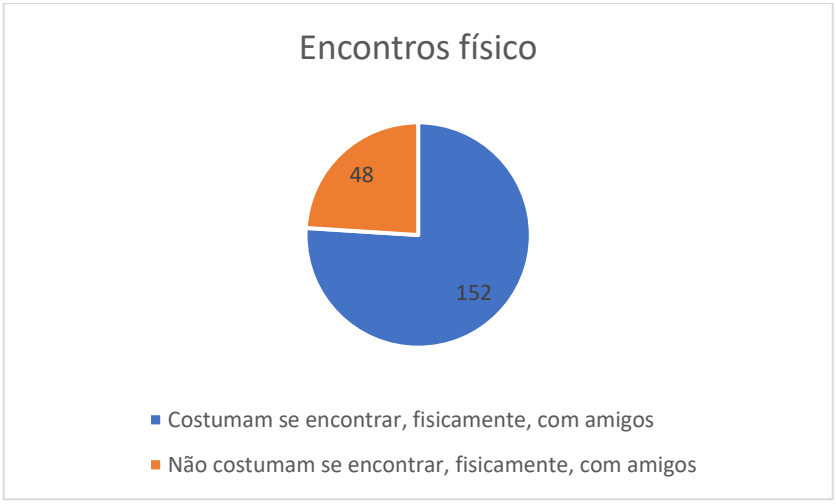


Gráfico 13 – Encontros físicos

A décima quarta pergunta formulada foi: O adolescente sai de casa de forma regular para ir a locais além da escola, para socializar? Os participantes tinham a opção de resposta de sim ou não. Vale ressaltar, outra vez, a preocupação com a interatividade física com outras pessoas, em ambiente diferente do escolar.

Os números trazidos foram de 138 para sim e 62 não. Em percentagem isso seria representado por 69% sim e 31% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que saem de suas casas para socializar com outras pessoas.

Costumam socializar além da escola	138
Não costumam socializar além da escola	62

Tabela 17 – Socialização além da escola

Gráfico 14 – Socialização além da escola

O quesito de número 15 (quinze) traz: O adolescente usa computadores ou *smartphone* no seu quarto? Sim ou não, eram as opções dada para a resposta. Vale ressaltar a importância de obter essa informação, já que o isolamento praticado pelos adolescentes, muitas vezes é com objetivo de evitar um maior monitoramento ou controle por parte de seus responsáveis legais.

O número de adolescentes que utilizam computadores ou *smartphones* dentro do quarto é de 173, e apenas 27 não utilizam neste ambiente, em regra. Em percentagem isso seria representado por 86,5% sim e 13,5% não.

A tabela e o gráfico a seguir mostram o número de adolescentes que utilizam computadores ou *smartphones* em seus quartos.

Usa computador ou smartphone no quarto	173
Não usa computador ou smartphone no quarto	27

Tabela 18 – Uso de Internet no quarto

Gráfico 15 – Uso de Internet no quarto

7.2.5 – Grupo 5 – Consciência (Responsável)

A décima sexta questão foi: O responsável sabe o que é cibercrime? Sendo respondido com sim ou não. Vale ressaltar que este questionamento terá por objetivo mostrar se, ao menos, o conceito amplo dos delitos praticados por meio da Internet é de conhecimento dos responsáveis.

São 169 os responsáveis que afirmam conhecer o conceito de cibercrimes e, 31 não conhecem. Em percentagem isso seria representado por 84,5% sim e 15,5 não.

A tabela e o gráfico a seguir mostram o número de responsáveis que conhecem ou não o conceito de cibercrimes.

Sabe o que são cibercrimes	169
Não sabe o que são cibercrimes	31

Tabela 19 – Conhecimento sobre cibercrimes

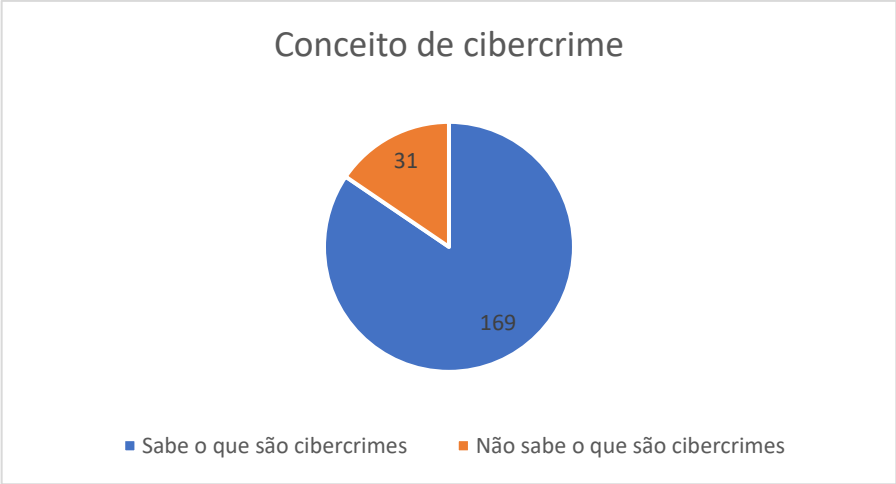


Gráfico 16 – Conhecimento sobre cibercrimes

O questionamento de número 17 (dezessete) traz: O responsável tem conhecimento que o adolescente já foi vítima de algum cibercrime? A resposta de sim ou não deveria ser dada. Vale ressaltar, a importância dessas informações, já que saber se o filho foi vítima de algum cibercrime fará com que providências e cuidados futuros sejam tomados.

O número de responsáveis que disseram que tinham conhecimento do filho ter sido vítima de cibercrimes foi de 170, por outro lado, 31 disseram que não. Em percentagem isso seria representado por 15% sim e 85% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que afirmam ter o conhecimento de que o filho foi ou não vítima de algum cibercrime.

Tem conhecimento que o filho foi vítima de algum cibercrime	30
Não tem conhecimento que o filho foi vítima de algum cibercrime	170

Tabela 20 – Conhecimento de vitimização do adolescente

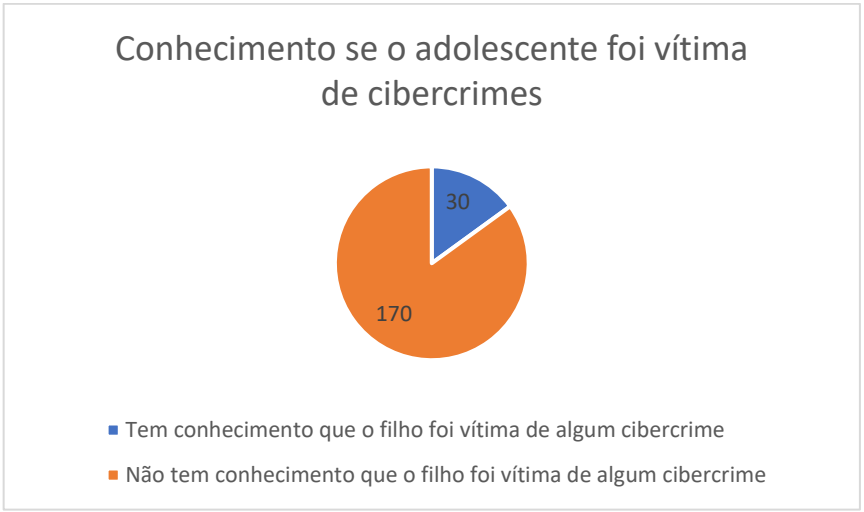


Gráfico 17 – Conhecimento de vitimização do adolescente

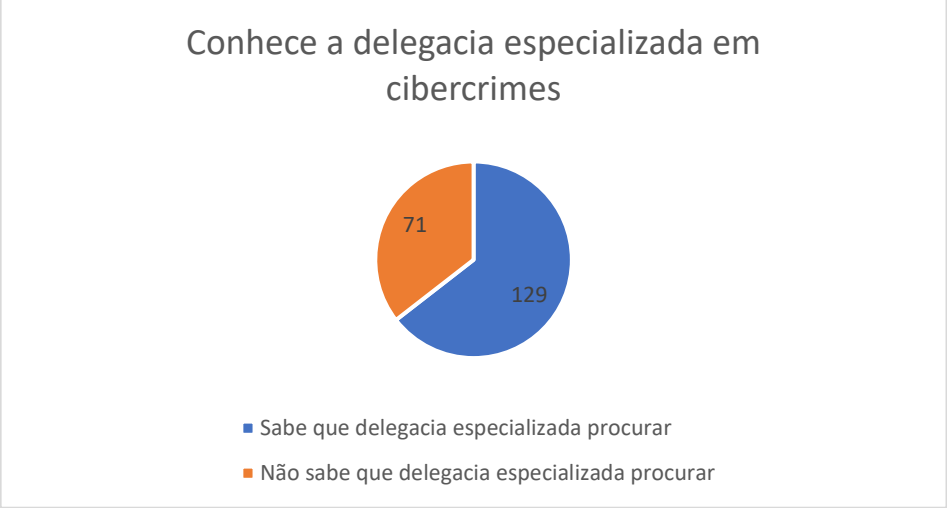
A pergunta 18 (dezoito) foi: O responsável sabe a que Delegacia de Polícia Civil Especializada a qual deve recorrer caso do adolescente seja vítima de cibercrimes? A opção de resposta era de sim ou não. Importante ressaltar que, esses dados nos mostrarão se o responsável sabe, ao menos, que delegacia especializada de Polícia Civil recorrer no caso de ter seu filho como vítima de cibercrimes, para não correr o risco de fazer procedimentos os quais não gerarão nenhum resultado.

O número de responsáveis que afirmaram saber a delegacia especializada para tratar de caso de cibercrimes é de 129 e, 71 afirmam que não sabem. Em percentagem isso seria representado por 64,5% sim e 35,5% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que afirmam sabe a delegacia especializada a qual devem recorrer em caso de seu filho ser vítima de algum cibercrime.

Sabe que delegacia especializada procurar	129
Não sabe que delegacia especializada procurar	71

Tabela 21 – Conhecimento sobre delegacia especializada em crimes cibernéticos



Gráfica 18 – Conhecimento sobre delegacia especializada em crimes cibernéticos

O décimo nono quesito abordou o seguinte: O responsável acha importante a divulgação sobre cibercrimes e cibersegurança nos meios de comunicações oficiais? Respondendo com sim ou não. A importância desse questionamento é para saber se, ao menos, o responsável tem preocupação em saber sobre um tema tão importante e sério na era contemporânea.

Os responsáveis que afirma ser importante a abordagem do tema nos meios de comunicações oficiais é de 189 e, 11 dizem que não. Em percentagem isso seria representado por 94,5% sim e 5,5% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que acham importante a divulgação dos temas de cibercrimes e cibersegurança nas mídias oficiais.

É importante o tema (cibercrime/cibersegurança) ser divulgado pelos meios de comunicações oficiais	189
Não é importante o tema (cibercrime/cibersegurança) ser divulgado pelos meios de comunicações oficiais	11

Tabela 22 – Importância da divulgação da temática cibercrimes e cibersegurança

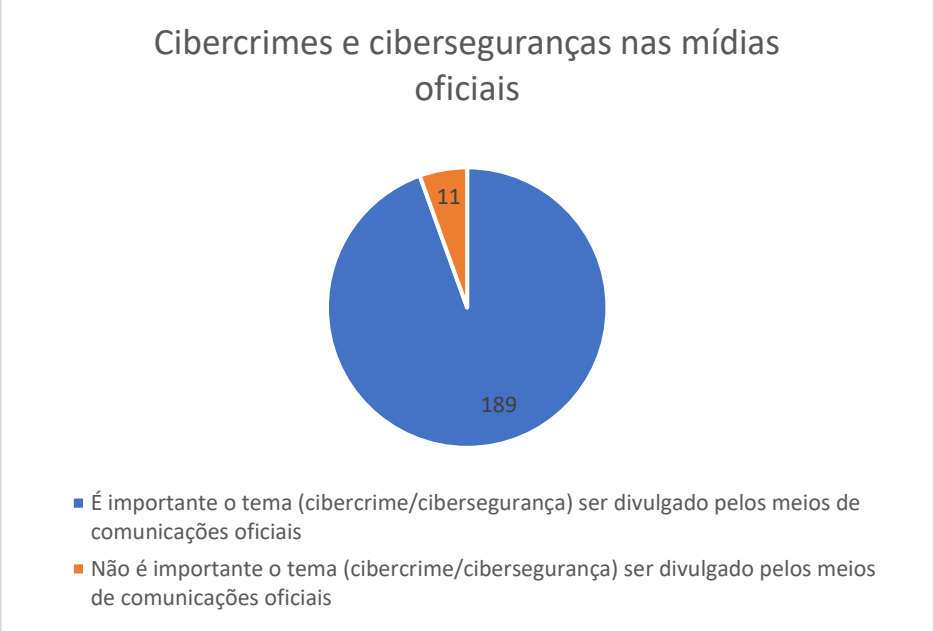


Gráfico 19 – Importância da divulgação da temática cibercrimes e cibersegurança

A pergunta de número 20 (vinte) é: O responsável acha importante as escolas abordarem tema como o cibercrime e a cibersegurança? Neste quesito foi respondido sim ou não. Vale ressaltar que, este questionamento irá mostrar o interesse dos responsáveis em ter a escola como parceira na prevenção e no combate dos cibercrimes.

O número de respostas contendo sim foram de 191, e não 11. Em percentagem isso seria representado por 95,5% sim e 4,5% não.

A tabela e o gráfico a seguir mostram o número de responsáveis os quais acham importante que o tema de cibercrimes e cibersegurança sejam tratados nas escolas.

É importante o tema (cibercrime/cibersegurança) ser tratado nas escolas	191
Não é importante o tema (cibercrime/cibersegurança) ser tratado nas escolas	9

Tabela 23 – Importância da temática cibercrimes e cibersegurança na escola

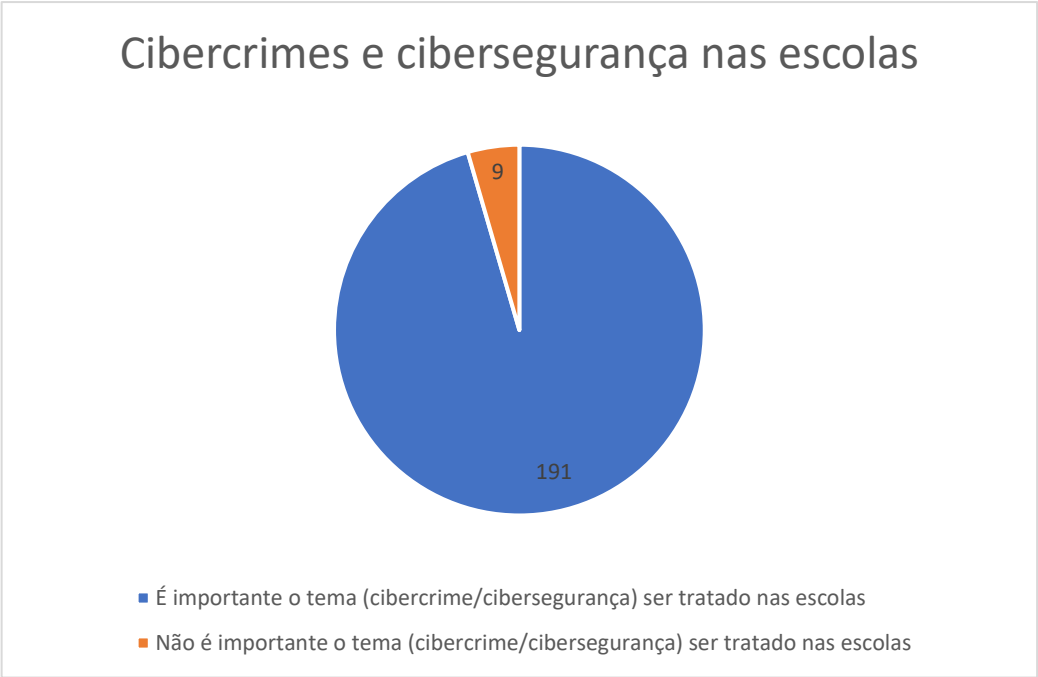


Gráfico 20 – Importância da temática cibercrimes e cibersegurança na escola

A última pergunta feita foi: O responsável gostaria de ter acesso a uma cartilha de instruções que mostra os principais cibercrimes e o modo de prevenção, voltado, especialmente, aos adolescentes? O participante tinha a opção de responder sim ou não. Vale salientar que, este questionamento irá mostrar a necessidade que o responsável tem de ter em suas mãos as devidas informações e orientações, para que possa prevenir e combater os cibercrimes, utilizando-se das ferramentas de cibersegurança, incluindo a orientação pessoal que pode ser dado ao seu filho.

Os responsáveis que responderam sim somaram 195, e os que não se interessam na cartinha, apenas 5. Em percentagem isso seria representado por 97,5% sim e 2,5% não.

A tabela e o gráfico a seguir mostram o número de responsáveis que se interessam em possuir uma cartilha onde terão informações sobre como prevenir seu filho para que este não venha a ser vítima em potencial dos cibercriminosos.

Gostaria de receber uma cartilha com dicas de prevenção contra cibercrimes	195
Não gostaria de receber uma cartilha com dicas de prevenção contra cibercrimes	5

Tabela 24 – Aceitação da cartilha de prevenção contra cibercrimes

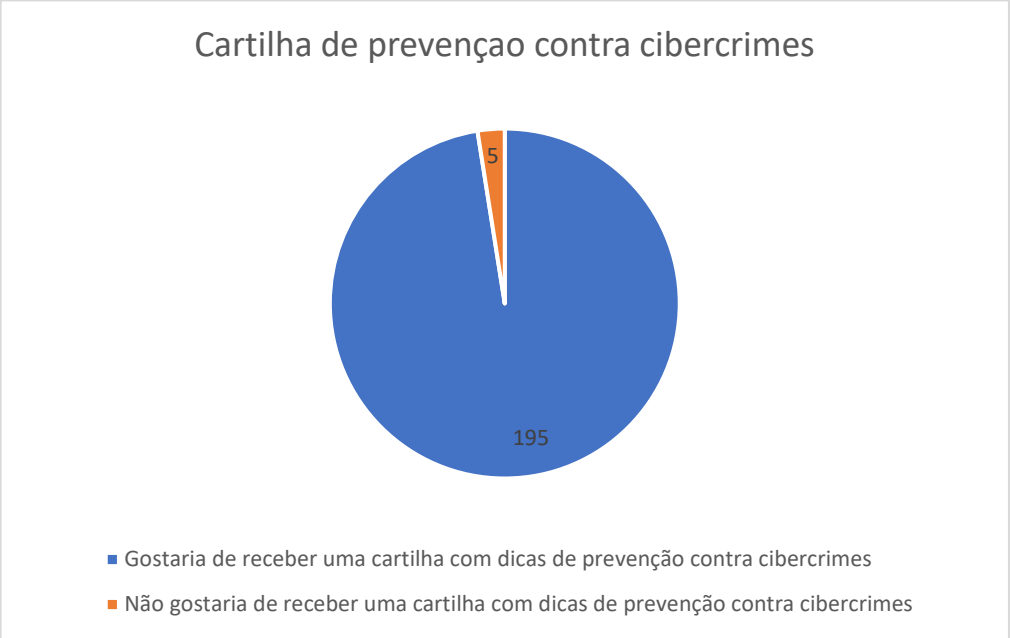


Gráfico 21 – Aceitação da cartilha de prevenção contra cibercrimes

7.3 – Recolha dos dados e o instrumento

A recolha dos dados foi realizada após ter sido aplicado como instrumento para tal tarefa, o preenchimento de questionários. Este chegou até o entrevistado de duas formas, quais sejam, por meio de link enviado pelo aplicativo de mensagens instantâneas (*WhatsApp*) e serviços de *emails*, onde ao clicar o participante era direcionado para a plataforma *Google Forms* e lá ia respondendo os quesitos. Em seguida, os dados eram copiados e colados em uma planilha do *Microsoft Excel*. A outra maneira foi a impressão, na integra, do questionário e a entrega para o participante, e após o preenchimento, os dados eram repassados manualmente para a planilha criada.

7.3.1 – Grupo 1 de perguntas

O primeiro grupo de questionamentos foi denominado Identificação e, está ligado ao adolescente, e é composto pelas perguntas 1 (um), 2 (dois) e 3 (três), quais sejam: pergunta 1 – Que idade tem o adolescente? A qual deve ser respondida com número inteiro que deve variar entre 12 e 17; pergunta 2 – Qual o gênero do adolescente? A qual deve ser respondido se masculino ou feminino, que para melhor trabalhar atribuímos o valor de 1 (um) para masculino e 0 (zero) para feminino; pergunta 3 – Que ano/curso frequenta o adolescente? Onde demos três opções, quais sejam: 1º grau que tem seu limite no 9º ano do ensino fundamental; 2º grau que é formado pelo 1º, 2º e 3º ano do ensino médio; ou curso profissionalizante, que pode ser os mais diversos, como por exemplo, mecânica, eletricista, confeitaria dentre outros, e nesta situação atribuímos o número 1 (um) para o 1º grau, 2 (dois) para o 2º grau e 3 (três) para cursos.

7.3.2 – Grupo 2 de perguntas

Ao segundo grupo de questionamentos chamamos de Conectividade e, está ligado ao adolescente, e é composto pelas perguntas 4 (quarto), 5 (cinco) e 6 (seis), quais sejam: pergunta 4 – O adolescente possui acesso à dispositivos conectados à Internet (*smartphone*, *tablet*, computador etc.)? A resposta será sim ou não, as quais foram atribuídos valores de 1 (um) para sim e 0 (zero) para não; pergunta 5 – O adolescente possui alguma rede social (Facebook, Instagram, WhatsApp etc.)? O entrevistado deve responder sim ou não, e foi atribuído valor de 1 (um) para sim e 0 (zero) para não; pergunta 6 – O adolescente possui acesso às suas contas em rede social? Somente tendo como alternativa, sim ou não. A resposta sim ganhará o valor 1 (um) e a não o valor 0 (zero).

7.3.3 – Grupo 3 de perguntas

Ao grupo número três de perguntas demos a nomenclatura Caracterização, a qual está diretamente ligada ao responsável pelo adolescente, isto é, o entrevistado. Neste, estão contidas as perguntas 7 (sete); 8 (oito), 9 (nove) e 10 (dez), vejamos: pergunta 7 – O responsável está ligado ou tem acesso às publicações nas redes sociais do adolescente? Tendo as opções de sim ou não, valorando o sim com número 1 (um) e o não com 0 (zero); pergunta 8 – Qual a escolaridade do responsável? Onde demos três opções, quais sejam: 1º grau que tem seu limite no 9º ano do ensino fundamental; 2º grau que é formado pelo 1º, 2º e 3º ano do ensino médio; ou nível superior, onde atribuímos o número 1 (um) para o 1º grau, 2 (dois) para o 2º grau e 3 (três) nível superior; pergunta 9 – O responsável faz o controle desse acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal? As opções de respostas foram sim ou não. Atribuímos valor 1(um) para sim e 0 (zero) para não; pergunta 10 – O responsável conhece todos os contatos virtuais do adolescente? As alternativas eram sim ou não, ganhando valor 1 (um) para sim e 0 (zero) para não.

7.3.4 – Grupo 4 de perguntas

Ao quarto grupo de perguntas demos o nome de Hábitos, e sua relação é diretamente com o adolescente. Este é formado por 5 (cinco) questionamentos, isto é, as perguntas de número 11 (onze), 12 (doze), 13 (treze), 14 (quatorze) e 15 (quinze), assim vejamos: pergunta 11 – Quanto tempo em média o adolescente fica conectado à Internet? Tendo como opção de resposta, sim ou não, onde o primeiro tem o valor 1 (um) e o segundo 0 (zero); pergunta 12 – O adolescente possui atividades extraescolares ou desporto, de forma frequente? As alternativas de marcação eram sim ou não, para sim o valor 1 (um) e para não 0 (zero); pergunta 13 – O adolescente possui um grupo de amigos regulares com quem se encontra fisicamente? Resposta composta pelas opções de sim ou não, para sim valoração 1 (um) e para não 0 (zero); pergunta 14 – O adolescente sai de casa de forma regular para ir a locais além da escola, para socializar? A resposta será sim ou não, as quais foram atribuídos valores de 1 (um) para sim e 0 (zero) para

não; pergunta 15 – O adolescente usa computadores ou *smartphone* no seu quarto? A resposta será sim ou não. Atribuímos valor 1(um) para sim e 0 (zero) para não.

7.3.5 – Grupo 5 de perguntas

O grupo 5 (cinco) recebeu o nome de Consciência, que está associado ao responsável pelo adolescente, isto é, as perguntas mostrar o quão consciente estes são em se tratando dos perigos que correm estes vulneráveis. Tal grupo é composto pelos quesitos 16 (dezesseis), 17 (dezessete), 18 (dezoito), 19 (dezenove), 20 (vinte) e 21 (vinte e um), assim dispostas: pergunta 16 – O responsável sabe o que é cibercrime? Como opção tínhamos sim ou não, que receberam valores de 1 (um) para sim e 0 (zero) para não. pergunta 17 – O responsável tem conhecimento que o adolescente já foi vítima de algum cibercrime? As alternativas eram sim ou não, valorada a primeira com 1 (um) e a segunda com 0 (zero). 18 – O responsável sabe a que Delegacia de Polícia Civil Especializada a qual deve recorrer caso do adolescente seja vítima de cibercrimes? As alternativas eram sim ou não, ganhando valor 1 (um) para sim e 0 (zero) para não. 19 – O responsável acha importante a divulgação sobre cibercrimes e cibersegurança nos meios de comunicações oficiais? Somente tendo como alternativa, sim ou não. A resposta sim ganhará o valor 1 (um) e a não o valor 0 (zero). 20 – O responsável acha importante as escolas abordarem tema como o cibercrime e a cibersegurança? Onde a resposta será sim ou não, tenho o valor 1 (um) para o sim e 0 (zero) para o não; pergunta 21 – O responsável gostaria de ter acesso a uma cartilha de instruções que mostra os principais cibercrimes e o modo de prevenção, voltado, especialmente, aos adolescentes? Tendo as opções de sim ou não, valorando o sim com número 1 (um) e o não com 0 (zero).

7.4 – Resumo do capítulo

Neste capítulo foram apresentados os dados recolhidos com base no questionário realizado de que resultaram 200 (duzentos) respostas de cada pergunta, como este é composto por 21 (vinte e um) perguntas, obtivemos 4.200 respostas, as quais foram divididas em 5 (cinco) grupos e que foram apresentados os resultados em forma de gráficos, assim como em números inteiros e percentuais.

Podemos verificar que, a idade média dos filhos dos participantes é de 14,4, o que implica em deduzirmos que está no meio da fase de adolescência, onde as mudanças comportamentais começam a se destacarem, fortemente.

A maioria dos entrevistados possuíam adolescente do sexo feminino e grau de escolaridade fundamental (1º grau). Por outro lado, todos adolescente possuem dispositivos que lhe dão conectividade com a Internet, onde 94,5% possuem rede social, e 64% ainda tem acesso as redes sociais de seus responsáveis.

Quando passamos a explorar o comportamento dos responsáveis, obtivemos o percentual de 80% que dizem ter acesso as publicações de seus filhos. Importante salientar que, 47,5% possuem nível superior. Ainda temos que 63,5% não conhecem os contatos virtuais dos adolescentes, o que nos deixam em alerta para análise posterior.

Extraímos uma informação fundamental que diz respeito ao tempo de conexão e, verificamos que o maior percentual, ou seja, 15,5% ficam em torno de 4 horas conectados. Quando tratamos das atividades extraescolares, isto é, longe das telas dos dispositivos e da Internet, obtivemos o resultado de que 74,5% dos adolescentes têm esse tipo de atividade, e que 76% costumam a se encontrar fisicamente com seus pares, e 69% socializam além do ambiente escolar.

Fomos mais além, queríamos saber se os adolescentes se mantinham em seus quartos quanto estavam acessando a Internet, e a resposta foi de que 86,5% ficam neste compartimento da casa, o que pode indicar um sinal de alerta.

Passamos a extrair dados relacionados ao conhecimento sobre cibercrimes. Assim, obtivemos que 84,5% dos participantes dizem conhecer este conceito e, que 85% não tem

conhecimento que o filho tenha sido vítima de um crime praticado por meios virtuais, onde 64,5% afirmam saber qual delegacia especializada procurar.

E, finalmente, quando foram questionados sobre o desejo de ter esse conhecimento sobre o assunto relacionado a cibercrimes e cibersegurança, verificamos que 94.5% acham importantes os meios de comunicações oficiais divulgarem informações esclarecedoras e até preventiva sobre o tema e, 95,5% gostariam que as escolas fossem a fonte dessas informações. Por fim, 97,5% gostariam de receber uma cartilha de cibersegurança contendo informações, conceitos e dicas de prevenção contra cibercrimes.

CAPÍTULO 8

ANÁLISES

8.1 – Introdução

Neste capítulo será realizada a análise dos dados que foram colhidos de acordo com os grupos de questões já estabelecidos. Assim, faremos o cruzamento dos dados que se encontram dentro do mesmo grupo, podendo tirar algumas conclusões adicionais.

Esta análise irá percorrer os seguintes grupos: Identificação, Conectividade, Caracterização, Hábitos e Consciência, onde em cada um desses, mostraremos os valores em percentual da análise, seguido de uma tabela e um gráfico para melhor visualização dos resultados.

No final desta análise, apresentaremos um quadro de resumo dos grupos de questões aplicadas, permitindo assim, um panorama geral e mais simplificado das análises e resultados obtidos.

Em seguida, faremos algumas considerações adicionais em relação aos resultados, estabelecendo ligações entre os dados encontrados em grupos diferentes, trazendo o que há de mais relevante e, mostrando que com o cruzamento de tais dados, podemos chegar a algumas conclusões que consideramos como relevantes para o presente estudo. Deve ser ressaltado que, neste tópico separamos os dados relacionados com os adolescentes do sexo masculino e feminino. Ainda, mostraremos gráficos com os valores, o que implica na facilitação da visualização e do entendimento por parte do leitor.

Logo após a análise, iremos trazer um tópico que tem por objetivo demonstrar a ligação que há entre as perguntas feitas no questionário aplicado e as perguntas e respostas trazidas pela cartilha, isto é, iremos mostrar o porquê as informações trazidas na cartilha são importantes para o conhecimento dos leitores. Para tal, tomaremos como base, os dados trazidos pela pesquisa realizada inicialmente.

De forma continuada, mostraremos os dados estatísticos do município de Belém, o qual foi realizada a pesquisa, trazendo o quantitativo populacional e, especificamente, de pessoas na faixa etária entre 12 e 17 anos.

Traremos, em seguida, as estratégias do governo brasileiro relacionadas com a segurança da informação, mostrando a legislação que definem as estratégias que deverão ser seguidas para a implementação de esquemas de cibersegurança.

Com objetivo de comparar, traremos dados relacionados à Portugal, no que diz respeito ao acesso à Internet dos adolescentes, exibindo os percentuais de conectividade, bem como as importantes participações de pais e responsáveis legais na condução de uma educação para a prevenção e redução de risco por via do acesso em excesso.

No final, mostramos o resumo de todo o capítulo, trazendo a principal informação recolhida no decorrer da análise feita, tanto nos grupos de forma individual como no cruzamento de dados efetuado. E ainda, traremos as devidas justificativas da composição da cartilha, tomando como base, as perguntas feitas no questionário aplicado aos pais e responsáveis dos adolescentes.

8.2 – Análise de dados relacionados à cibersegurança

Será apresentada a análise dos resultados, tomando as questões de acordo com os grupos às quais estas pertencem e que foram previamente apresentados. Assim, poderemos obter uma visão geral melhor e, em seguida, mais condições de fazer o cruzamento desses dados, com o objetivo de obter evidências com potencial de explicarem os fenômenos estudados durante o desenvolvimento do trabalho e que estão associados com o uso e exploração de meios digitais, por jovens, com foco nos riscos associados.

8.2.1 Análise de questões do grupo 1: Identificação

No primeiro grupo de questionamentos foram obtidos os dados relacionados com o adolescente, isto é, idade, gênero e grau de escolaridade. Assim, podemos verificar que de acordo com a média das idades, estes estão cursando a série escolar condizente, isto é, estão dentro de uma regularidade no que diz respeito à relação idade versus escolaridade. Tal análise, nos mostra que a maturidade dos adolescentes está acompanhando o desenvolvimento cerebral no âmbito relacionado à educação, o que é de relevante importância, tendo em mente que um aluno com idade avançada que participa ainda de séries inferiores a que deveria frequentar, pode ter problemas no avanço cognitivo e intelectual, fazendo com que a sua maturidade demore ainda mais a se desenvolver, tornando-o assim, mais vulnerável às ocorrências como vítima de cibercrimes.

A tabela a seguir mostra claramente as nossas conclusões relacionadas com os fatores: idade versus escolaridade.

Idade	Quantidade de Adolescentes	Escolaridade
12	41	1º grau
13	29	1º grau
14	31	1º grau
14	6	2º grau
15	14	1º grau
15	16	2º grau
16	6	1º grau
16	21	2º grau
17	5	1º grau
17	27	2º grau
17	4	Curso Profissionalizante

Tabela 25 - Idade versus escolaridade

Inferimos que, o grau de escolaridade nos mostrará que as instruções obtidas por meio das escolas estão em um patamar de simetria com relação às idades. Assim, podemos concluir que o comportamento desse público deve indicar o nível de vulnerabilidade no que diz respeito a possibilidade de serem vitimados pelos cibercriminosos, devido ao comportamento destes ao navegar no mundo virtual.

8.2.2 Análise de questões do grupo 2 – Conectividade

Do segundo grupo de perguntas conseguimos extrair mais alguns dados relacionados diretamente aos adolescentes, que são: acesso à Internet, redes sociais e acesso a contas de redes sociais dos seus responsáveis.

Conforme já esperávamos, a crescente evolução da tecnologia e, principalmente, a diversidade trazida de atividades, sejam laborais ou entretenimento, dificilmente deixaria o adolescente de fora de tal universo, por isso, 100 % dos participantes afirmaram que os seus têm acesso a dispositivos conectados à rede mundial de computadores.

Entre os adolescentes que possuem acesso à Internet, há um dado ainda mais alarmante, 94,5% possuem redes sociais, ainda que, em regra, estas exijam a maior idade (18 anos no Brasil), e ainda extraímos que 64% possuem acesso a conta das redes sociais de seus responsáveis legais, o que permite ter um acesso a conteúdo próprios para adultos, tornando-os, assim, presas facilmente atraídas pelos cibercriminosos, tendo em vista que o potencial cognitivo de autoafirmação pode levar aos perigos do ciberespaço.

Possui acesso a dispositivo conectado à Internet	100%
Possui rede social	94,50%
Possui acesso a rede social do responsável	64%

Tabela 26 – Combinação de dispositivos com acesso à Internet e acesso ou não de rede social

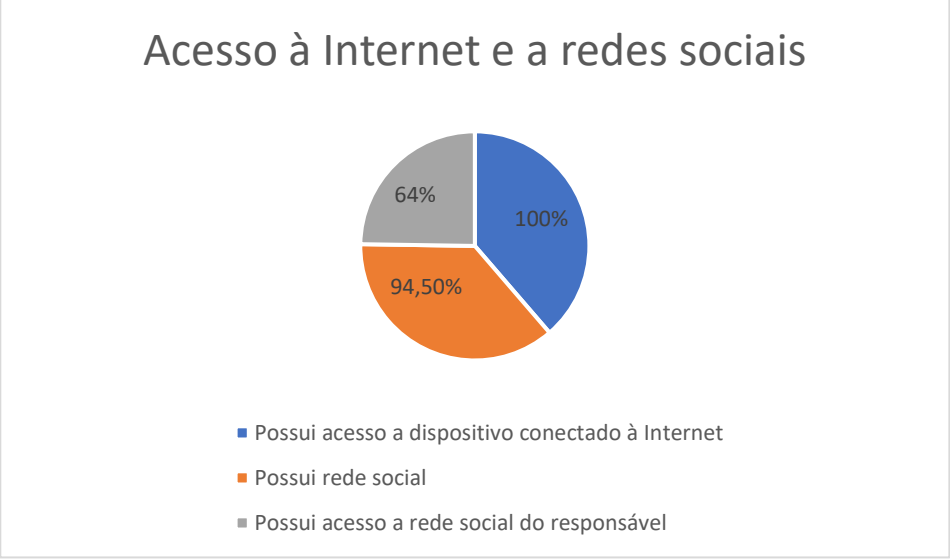


Gráfico 22 – Combinação de dispositivos com acesso à Internet e acesso ou não de rede social

Importante salientar que, o acesso à Internet feito pelos adolescentes versus o uso de redes sociais, nos levam a concluir que estes basicamente utilizam estes meios de interações como principal ferramenta, já que a grande maioria, ou possui uma conta ou tem acesso à conta dos seus responsáveis. No entanto, verificamos que apenas 9 dos 200 participantes afirmam que os seus filhos não têm rede social e nem acesso às suas contas, o que os tornam menos vulneráveis, porém, não blindados aos cibercrimes.

Não acesso à Internet e não possui nenhum tipo de acesso à rede social	4,5%
Possui acesso à Internet e a rede social	95,5%

Tabela 27 – Acesso à Internet com ou sem acesso a rede social

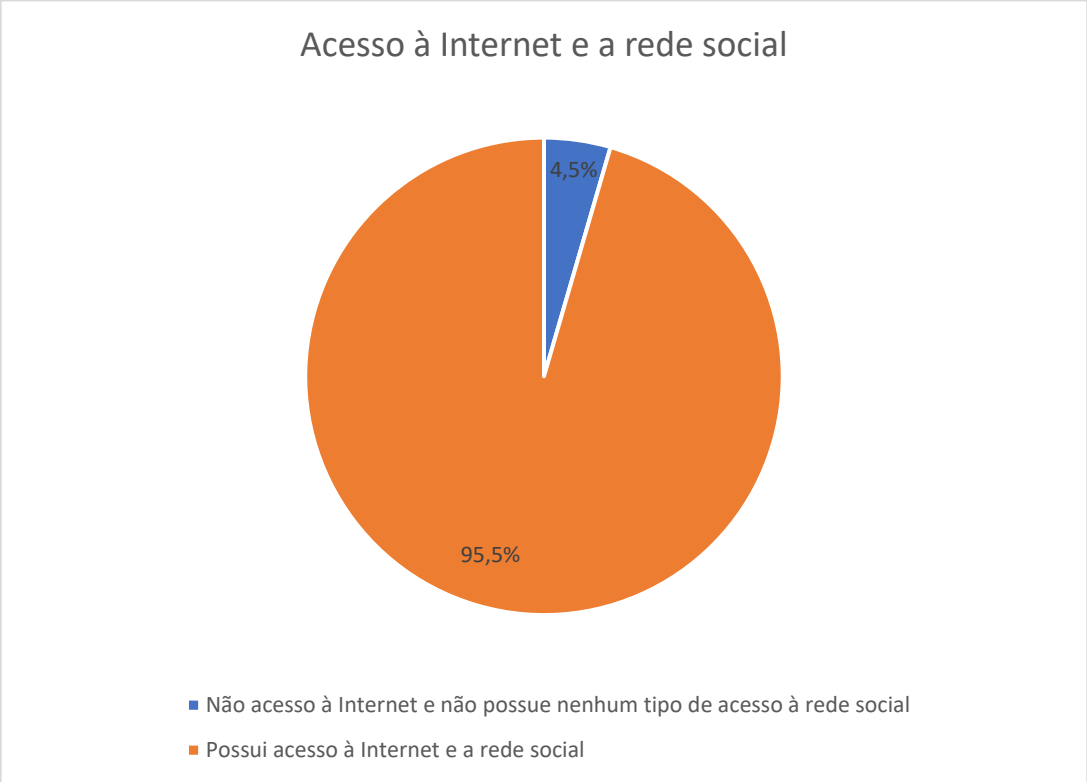


Gráfico 23 – Acesso à Internet com ou sem acesso a rede social

Ao final inferimos que, um baixo percentual de adolescentes não possui qualquer contato com redes sociais. No entanto, devemos ter em mente que a mentira é fator característico na adolescência, fazendo assim, com que deduzamos o acesso destes, ainda que com perfil falso. Pois, é bem difícil ser aceito por seus pares, sem a participação nesta forma virtual de entretenimento.

8.2.3 – Análise de questões do grupo 3 – Caracterização

Do terceiro grupo de perguntas extraímos que 15% dos responsáveis não estão ligados nas publicações de seus adolescentes e nem fazem nenhum tipo de controle de monitoramento, seja pessoal ou através de software específicos.

Retiramos que, 15,5% dos participantes possuem nível fundamental (1º grau), e desses, teremos 93,87% afirmando estarem ligados nas publicações de seus filhos. Encontramos, ainda, o resultado de 87,09% que fazem o controle do acesso, através de programas ou monitoramento pessoal. E, finalmente, 80,64% conhecem os contatos virtuais dos seus adolescentes.

Ligados nas publicações do adolescente	93,87%
Controlam o acesso do adolescente	87,09%
Conhecem os contatos virtuais do adolescente	80,64%

Tabela 28 – Combinação entre nível fundamental, publicações, controle e contatos virtuais

Gráfico 24 – Combinação entre nível fundamental, publicações, controle e contatos virtuais

Extraímos que, 37% dos participantes possuem nível médio (2º grau), e desses, temos 75,67% que afirmam estarem atentos às publicações feitas pelos seus filhos. Ainda encontramos o resultado de 62,16% que controlam o acesso, ou por meio de programas ou monitoramento pessoal. E, finalmente, 31,08% conhecem os contatos virtuais dos seus adolescentes.

Ligados nas publicações do adolescente	75,67%
Controlam o acesso do adolescente	62,16%
Conhecem os contatos virtuais do adolescente	31,08%

Tabela 29 – Combinação entre nível médio, publicações, controle e contatos virtuais

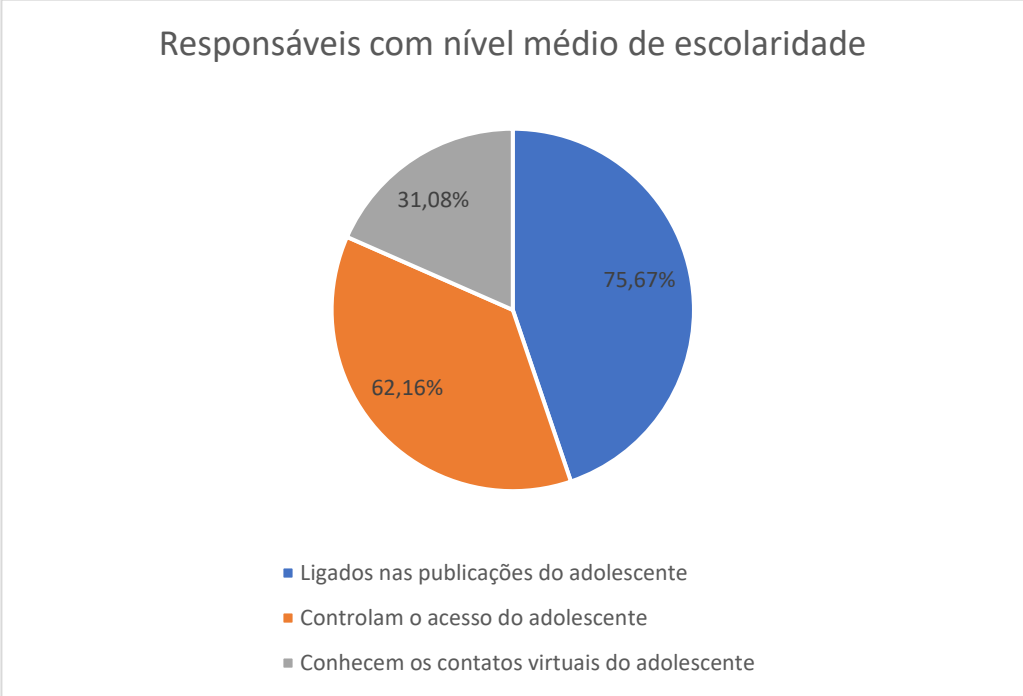


Gráfico 25 – Combinação entre nível médio, publicações, controle e contatos virtuais

Percebemos que, 47,5% dos participantes possuem nível superior, e desses, temos 82,10% que afirmam estarem atentos as publicações feitas pelos seus filhos. Ainda chegamos ao resultado de 72,63% que fazem algum tipo de controle no acesso, ou por meio de programas ou monitoramento pessoal. E, finalmente, 26,31% conhecem os contatos virtuais dos seus adolescentes.

Ligados nas publicações do adolescente	82,10%
Controlam o acesso do adolescente	72,63%
Conhecem os contatos virtuais do adolescente	26,31%

Tabela 30 – Combinação entre nível superior, publicações, controle e contatos virtuais

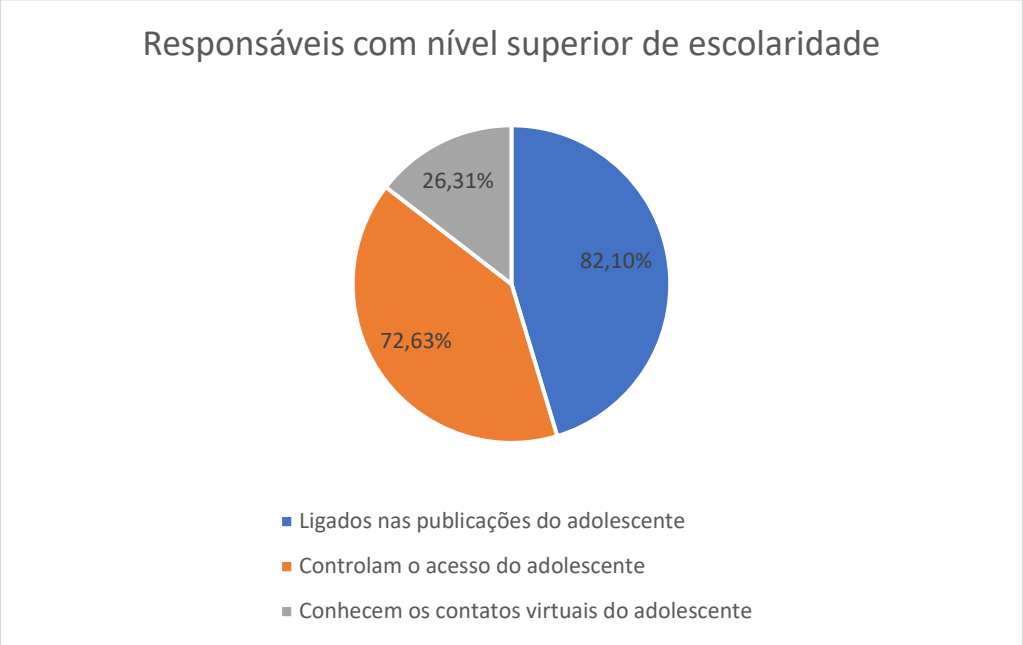


Gráfico 26 – Combinação entre nível superior, publicações, controle e contatos virtuais

Após os números mostrados podemos concluir que, apesar, dos responsáveis afirmarem que observam as postagens do adolescente e, que tem algum controle sobre o acesso dos seus, estes na maioria não conhecem os contatos. Tal, implica um perigo real, pois muitos cibercriminosos criam perfis falsos para atraírem as suas vítimas, e as ideias trocadas podem mostrar a malícia que há por trás, todavia, só com uma maior experiência é que pode ser percebido.

8.2.4 Análise de questões do grupo 4 – Hábitos

A extração feita no grupo 4, foi de que 24% dos adolescentes não têm encontros físico regulares com amigos. Isso nos mostra que, cada vez mais, está ocorrendo o afastamento deste tipo de contato o qual é tão importante. E é notório que o ambiente virtual é um vilão neste afastamento.

Foi, também, obtido o percentual de 31% que não saem de casa para frequentar outros ambientes, diferentes da escola. E o mais preocupante é que 86,5% utilizam os seus dispositivos dentro dos seus quartos, o que nos mostra a facilidade de esconder toda e qualquer prática

inapropriada no acesso à Internet, o que, ainda, pode deixar mais vulnerável e difícil de fazer o controle dessa navegação.

Não possuem encontros físicos, regulares, com amigos	24%
Não frequentem outros ambientes além da escola	31%
Utilizam dispositivos conectados à Internet dentro do quarto	86,5%

Tabela 31 – Combinação entre encontro físico, ambiente extraescolar e acesso à Internet dentro do quarto

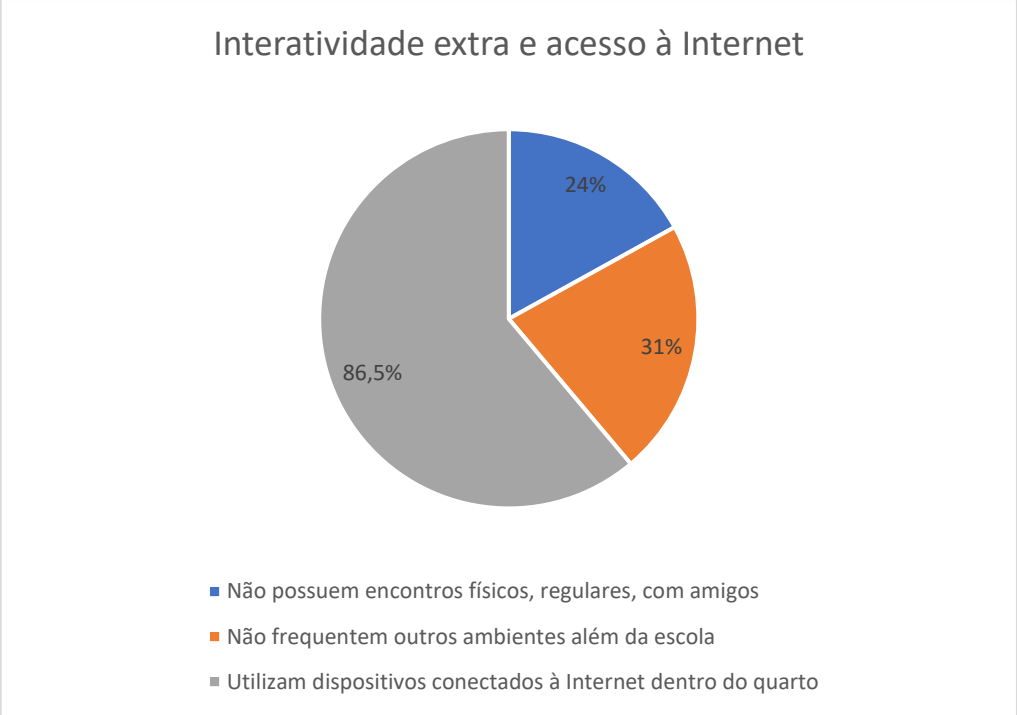


Gráfico 27 – Combinação entre encontro físico, ambiente extraescolar e acesso à Internet dentro do quarto

Inferimos que, os adolescentes, na maioria, possuem alguma forma de interatividade com os seus pares. Por outro lado, o que nos parece é, que cada vez mais eles utilizam lugares reservados para acessar à Internet, e é aí que surge o perigo, pois longe do monitoramento é mais fácil eles serem vítimas de cibercriminosos. Vale ressaltar que, dificilmente, eles informarão aos responsáveis, o facto ocorrido, afinal, eles se acham preparados para viver a vida sem orientações dos mais experientes.

8.2.5 – Análise de questões do grupo 5 – Consciência

Ao analisarmos o grupo 5, o qual é de extrema importância, inclusive, para realização da proposta final da nossa tese, verificamos que 70,5% dos participantes, apesar de afirmarem que sabem o que é cibercrimes, estes não têm conhecimento se seu filho (a) já foi vítima de tal ato. Isso nos mostra que, muitas vezes, não há uma relação de confiança entre os pais e os filhos, além de demonstrar que o monitoramento dos adolescentes, se faz essencial para detectar qualquer que seja a suspeita de cibercrimes e, assim, poder agir de forma que não venha a se concretizar este ato criminoso, e nem atinja, principalmente, o psicológico do adolescente.

Ao questionar sobre a importância da divulgação do tema cibercrimes e cibersegurança e, ainda, extrair o interesse dos responsáveis em tem uma cartilha para que possam ter o conhecimento e assim ajudar seus filhos, orientando-os, para que não sejam vitimados pelos cibercriminosos, é de 92% de aceitação. Ressaltamos que, este resultado mostra o quanto é interessante, bem como, o tamanho da preocupação dos responsáveis em saber mais sobre um tema tão atual, o qual vem fazendo vítimas no mundo inteiro e, o que é pior, causando sérios danos, tanto físico quanto psicológicos, transformando, assim, nossa população adolescente em pessoas vulneráveis e com grande propensão para entrarem na estatística de vítimas de cibercrimes.

Não sabem o que é cibercrimes	70,5%
Gostariam de ter uma cartilha explicativa sobre o tema cibercrimes e cibersegurança	92%

Tabela 32 – Combinação entre conhecimento de cibercrimes e interesse na cartilha de prevenção

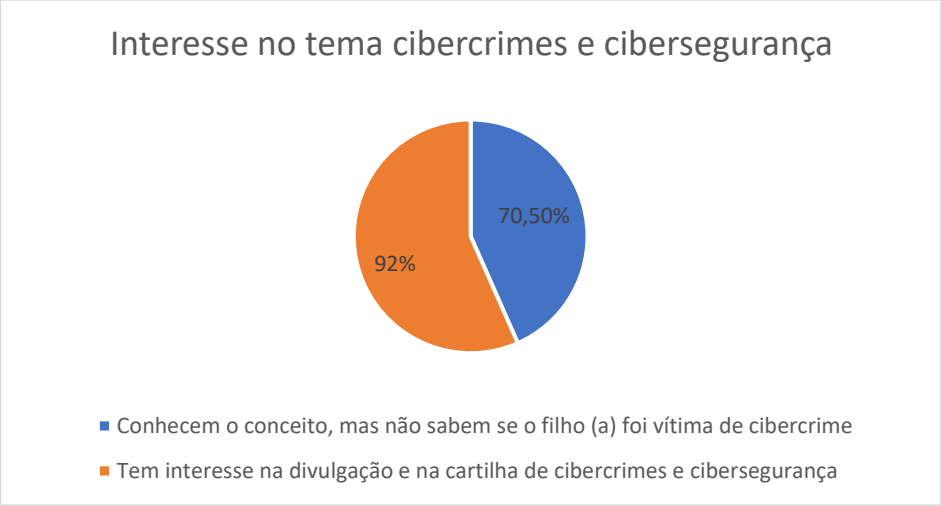


Gráfico 28 – Combinação entre conhecimento de cibercrimes e interesse na cartilha de prevenção

Neste grupo de questionamentos percebemos que, a aceitação de ter mais conhecimento sobre o assunto relacionado com os cibercrimes e cibersegurança é da esmagadora maioria, isto é, aqui podemos ver a carência que os responsáveis têm em ter essa consciência, para posteriormente, passar aos seus adolescentes. Ressaltamos, aqui, a contribuição que este trabalho pode vir a ter, e o quão relevante é este contributo para a ajudar a sociedade no enfrentamento um problema tão atual e que pode trazer consequências drásticas para os nossos adolescentes.

8.3 – Quadro resumo com o essencial da análise por grupos de questões

Mostraremos um quadro com resumo de toda a análise relacionadas aos grupos os quais foram divididas as perguntas encontradas no questionário aplicado aos responsáveis por adolescente. Logo, os dados apresentados representam as combinações que achamos coerentes, levando em consideração somente o grupo de perguntas encontrado em cada grupo.

GRUPOS	DESCRIÇÃO	DADOS
Grupo 1 – Identificação	1º grau	126
	2º grau	70
	Curso Profissionalizante	4
Grupo 2 – Conectividade	Possuem acesso à Internet	94,50%
	Possuem acesso a redes sociais dos responsáveis	64%
	Não possuem acesso à Internet e nem a redes sociais	4,50%
	Possuem acesso à Internet e a redes sociais	95,50%
Grupo 3 – Caracterização	Responsáveis com nível fundamental e ligados nas publicações do filho (a)	93,87%
	Responsáveis com nível fundamental e que controlam o acesso do filho (a)	87,09%
	Responsáveis com nível fundamental e conhecem contatos virtuais do filho (a)	80,64%
	Responsáveis com nível médio e ligados nas publicações do filho (a)	75,67%
	Responsáveis com nível médio e que controlam o acesso do filho (a)	62,16%
	Responsáveis com nível médio e conhecem contatos virtuais do filho (a)	31,08%
	Responsáveis com nível superior e ligados nas publicações do filho (a)	82,10%

	Responsáveis com nível superior e que controlam o acesso do filho (a)	72,63%
	Responsáveis com nível superior e conhecem contatos virtuais do filho (a)	26,31%
Grupo 4 – Hábitos	Adolescentes que não possuem encontros físicos, regulares, com amigos	24%
	Adolescentes que não frequentem outros ambientes além da escola	31%
	Adolescentes que utilizam dispositivos conectados à Internet dentro do quarto	86,5%
Grupo 5 – Consciência	Não sabem o que é cibercrimes	70,5%
	Gostariam de ter uma cartilha explicativa sobre o tema cibercrimes e cibersegurança	92%

Tabela 33 – Resumo das combinações de dados

8.4 – Considerações adicionais sobre os resultados

Faremos algumas combinações de questionamentos que se encontram em grupos diferentes de modo a extrair mais alguns pontos de análise relevantes para o nosso estudo.

8.4.1 – Análise de conhecimento de contato e controle de acesso do sexo feminino

Os dados relacionados com o sexo feminino mostram que dos 114 participantes, 79 afirmam que fazem o controle do acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal, e isso corresponde a 69,30%. Ainda temos que, 35 não fazem tal controle, o que implica em 30,70%.

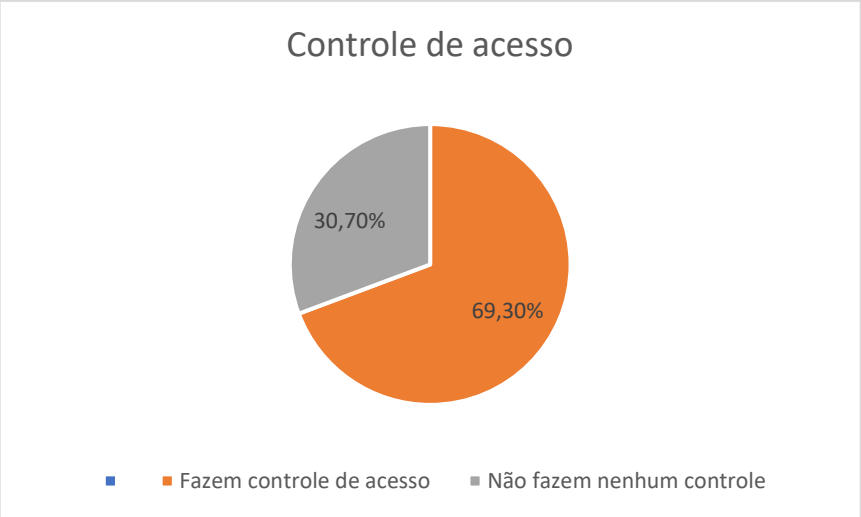


Gráfico 29 – Controle de acesso de adolescente do sexo feminino

Ao tratarmos do questionamento relacionado com o conhecimento dos contatos das adolescentes, temos que, 42 participantes afirma conhecer todos os contatos virtuais, o que significa 36,84%. E aqueles que dizem não conhecer, chegam ao número de 72 participante, o que representa 63,16%.

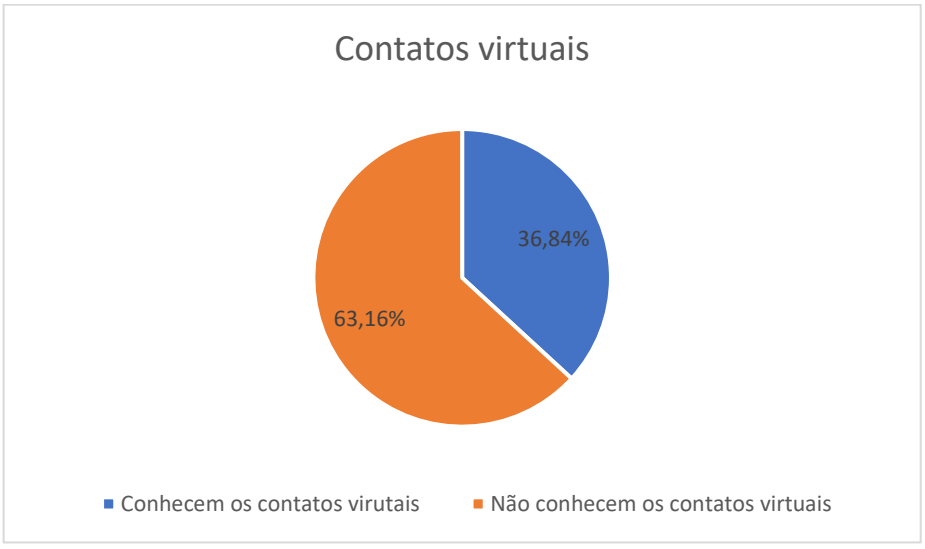


Gráfico 30 – Contatos virtuais de adolescente do sexo feminino

Seguimos fazendo combinações, e chegamos ao valor de 40 participantes, isto é, 35,08% que fazem o controle ou monitoramento, porém, não conhecem todos os contatos virtuais das suas adolescentes.

Quando analisamos os responsáveis que fazem o controle ou monitoramento e conhecem todos os contatos das adolescentes, chegamos ao quantitativo de 39 participante, o que implica em 34,21%.

Ao cruzarmos os dados dos responsáveis que não fazem nenhum controle ou monitoramento e que não conhecem todos os contatos das adolescentes, chegamos ao número de 32, o que representa 28,07%.

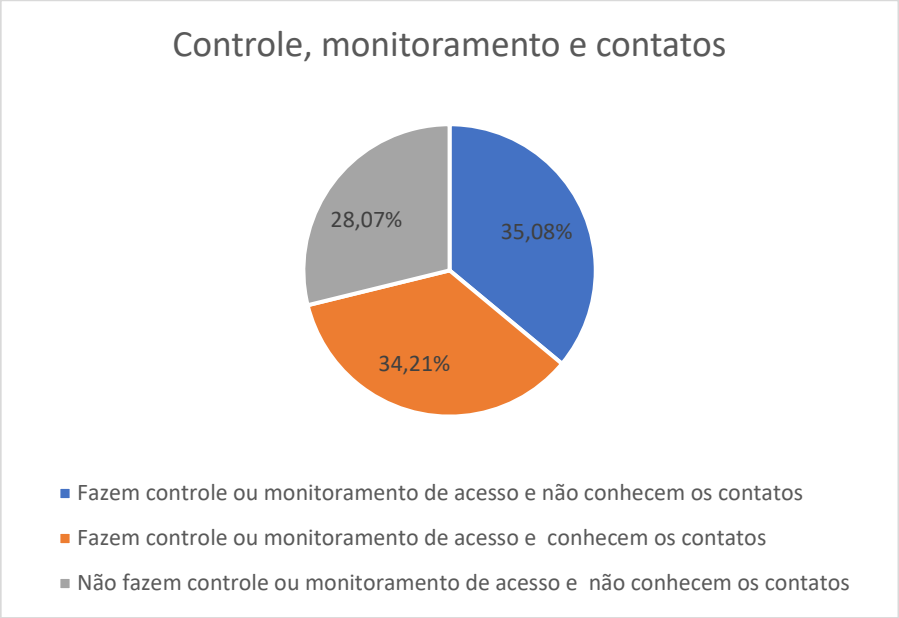


Gráfico 31 – Combinação entre controle, contatos virtuais de adolescente do sexo feminino

8.4.2 – Análise de conhecimento de contato e controle de acesso do sexo masculino

A recolha e análise dos dados do sexo masculino mostram que dos 86 participantes, 63 afirmam que fazem algum tipo de controle do acesso à Internet, usando programas específicos de segurança ou monitoramento pessoal, e isso corresponde a 73,25%. Ainda colhemos que, 23 não fazem qualquer controle, o que implica uma existência de 26,75% - quase um terço das participantes.

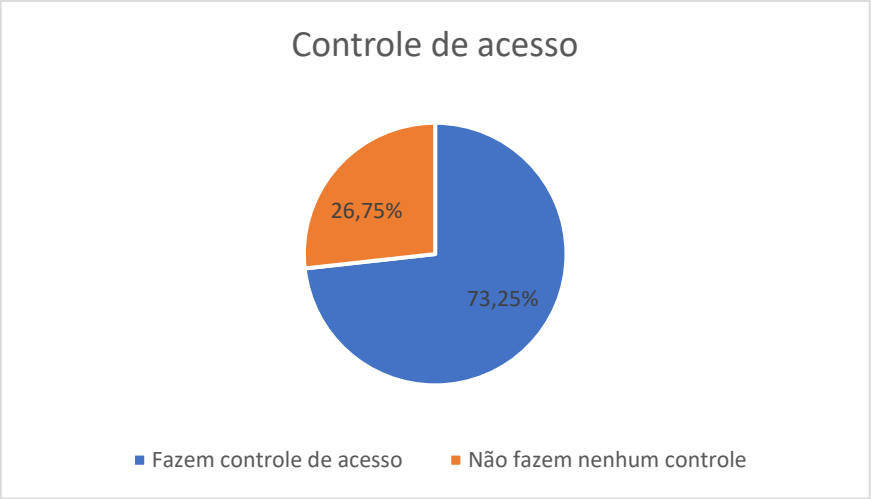


Gráfico 32 – Controle de acesso de adolescente do sexo masculino

Em relação ao questionamento sobre o conhecimento dos contatos dos adolescentes, temos que, 31 participantes afirmam conhecer todos os contatos virtuais, o que significa 36,05%. E os que dizem não conhecer, somam 55 participantes, o que representa 63,95%.

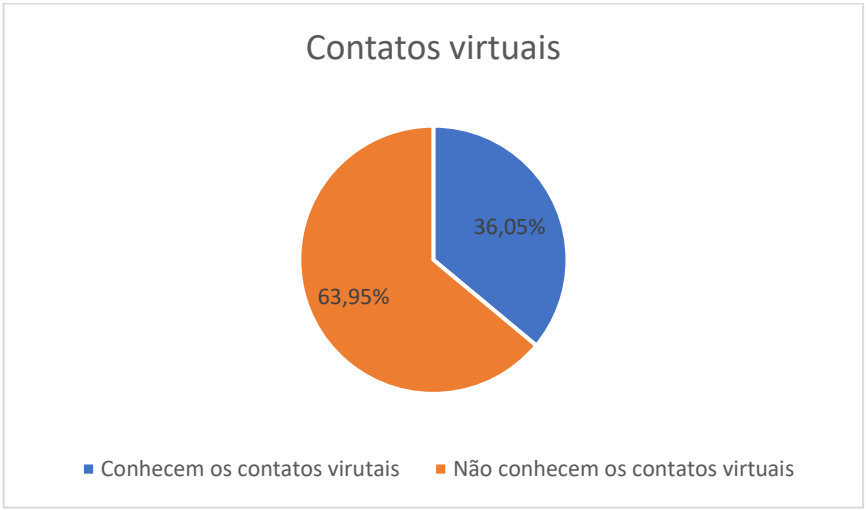


Gráfico 33 – Contatos virtuais de adolescente do sexo masculino

Dando continuidade às combinações, chegamos ao total de 33 participantes, isto é, 38,37% que fazem o controle ou monitoramento, no entanto não conhecem todos os contatos virtuais das suas adolescentes.

Quando fizemos a análise dos responsáveis que fazem o controle ou monitoramento e que conhecem todos os contatos das adolescentes, chegamos ao quantitativo de 30 participante, o que implica em 34,88% – aqui, claramente um terço das participantes no estudo.

Ao fazermos o cruzamento de dados dos responsáveis que não fazem nenhum controle ou monitoramento e, também, não conhecem todos os contatos das adolescentes, chegamos ao número de 22, o que representa 25,58% – cerca de um quarto do total.

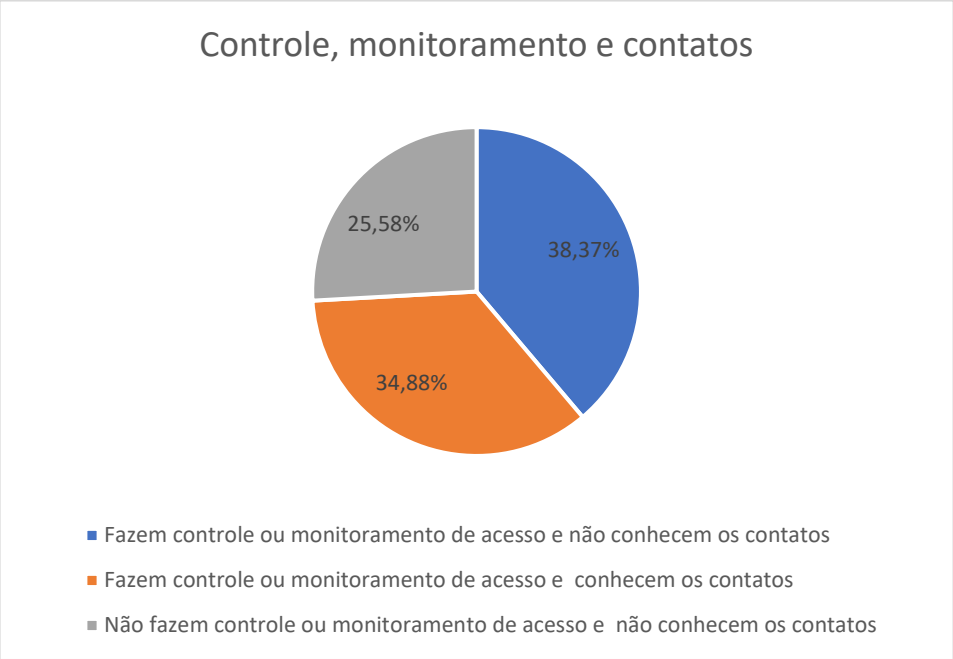


Gráfico 34 – Combinação entre controle, contatos virtuais de adolescente do sexo masculino

8.4.3 – Análise de interatividades fora do ambiente virtual dos adolescentes do sexo feminino

Ao fazermos a análise relacionadas com as atividades extraescolares, obtivemos os resultados de, 85 adolescentes do sexo feminino que as fazem, o que corresponde a 74,56%, enquanto 29 não possuem outras atividades além da escolar, representando 25,44%.

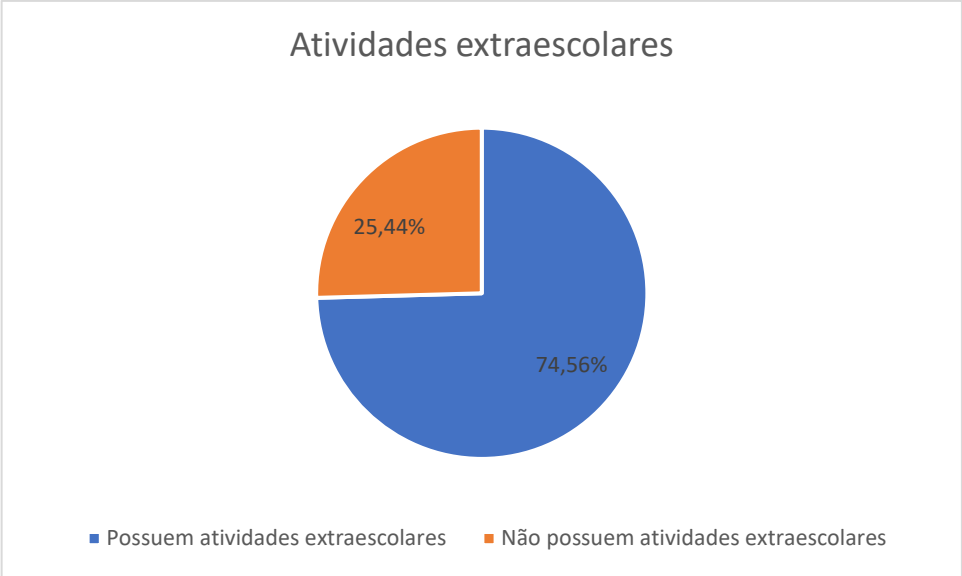


Gráfico 35 – Atividades extraescolares de adolescente do sexo feminino

Quando o questionamento passou a ser sobre possuir ou não grupo de amigos que se encontram regularmente, obtivemos os valores de 87 afirmando que sim e 27 não, o que corresponde a 76,31% e 23,69%, respectivamente.

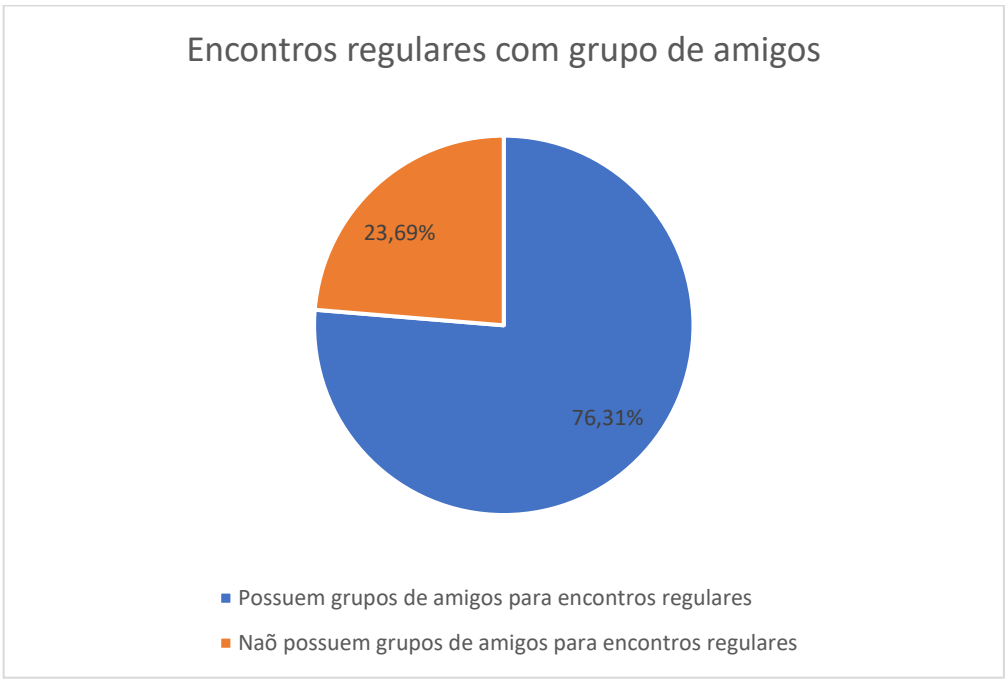


Gráfico 36 – Encontro físicos regulares de adolescente do sexo feminino

Com relação a frequentar ou não lugares além da escola, de forma regular, obtivemos os números de 76 que disseram sim, equivalendo a 66,66% e, 38 disseram que não frequentam outros lugares, regularmente, sendo este equivalente a 33,34%.

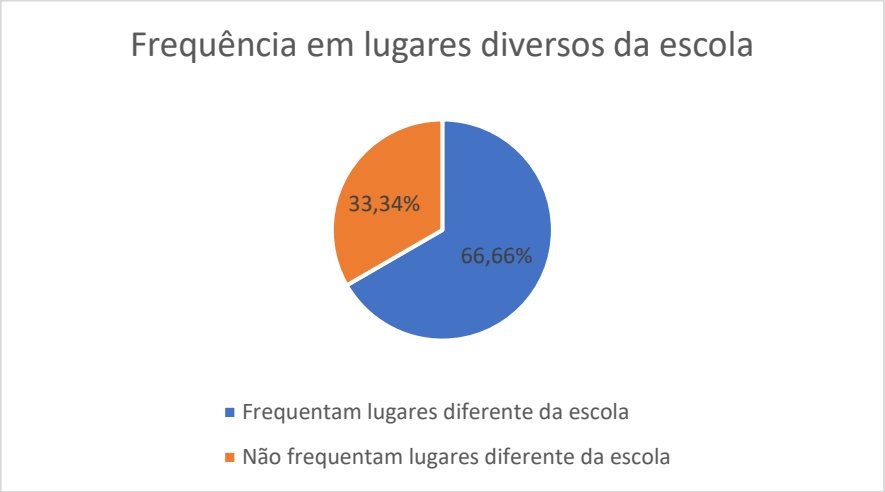


Gráfico 37 – Frequência em lugares diversos da escola de adolescente do sexo feminino

Ao analisar os dados, observamos que 53 adolescentes femininas têm atividade extraescolar, possuem grupos de amigos para encontros regulares e saem de casa para socializar em outros locais, fisicamente. Em percentual teremos o valor de 46,49%.

Por outro lado, temos 6 participantes feminino que não possuem atividades extraescolares, nem possui amigos para encontros físicos e não sai para lugares diferentes da escola para socializar. Isso corresponde a 5,26%.

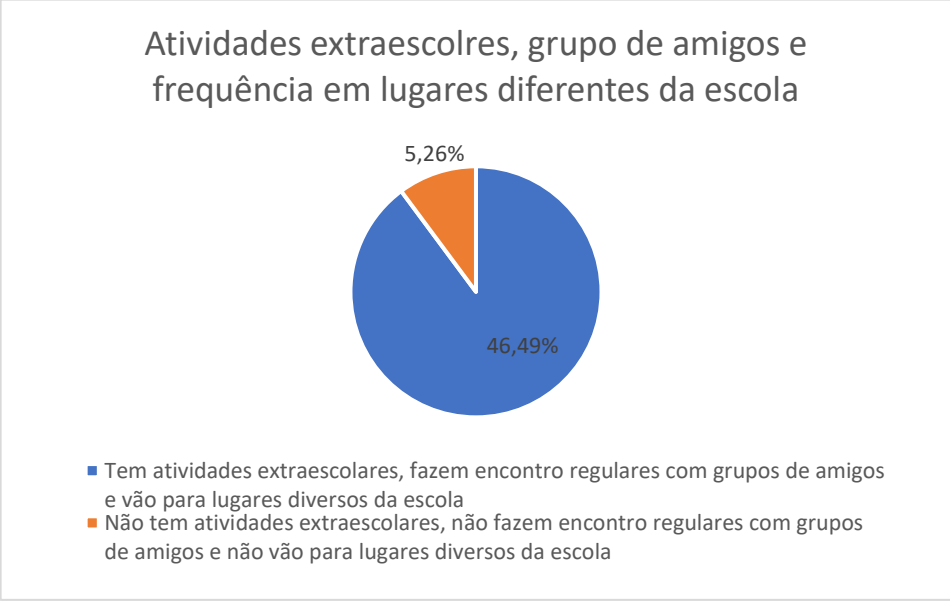


Gráfico 38 – Combinação entre atividades extraescolares, encontros físicos e lugares diversos da escola de adolescente do sexo feminino

8.4.4 – Análise de interatividades fora do ambiente virtual dos adolescentes do sexo masculino

Ao serem analisados os dados relacionados a atividades extraescolares, obtivemos como resultado que 64 adolescentes do sexo masculino as realizam, o que corresponde a 74,42%, enquanto 22 não possuem atividades além da escolar, representando 25,58%.

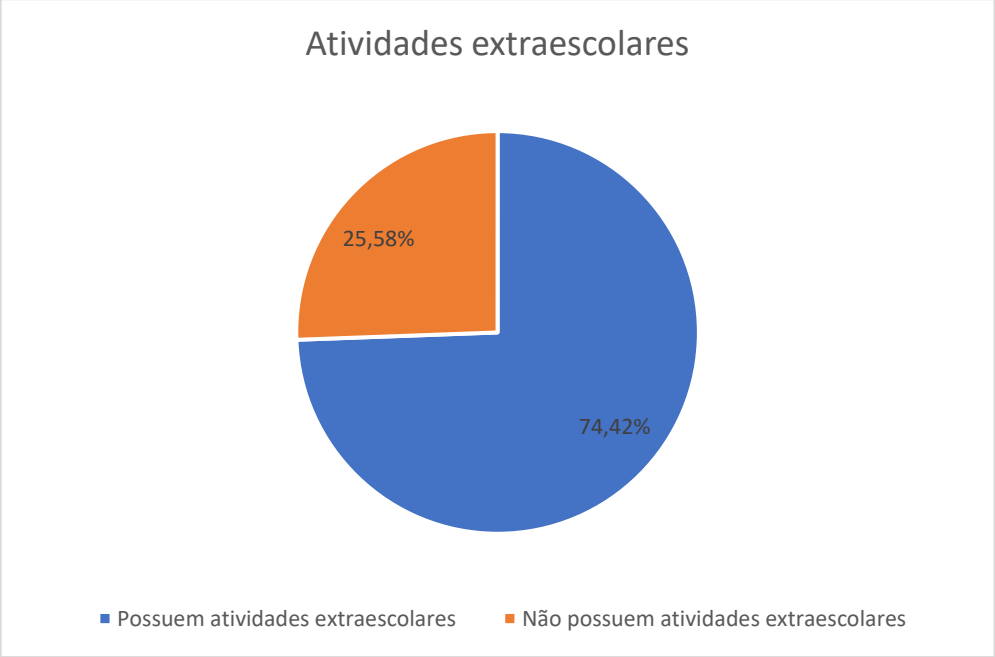


Gráfico 39 – Atividades extraescolares de adolescente do sexo masculino

Quando passamos para questão de possuir ou não grupo de amigos que se encontram regular e fisicamente, foram obtidos os valores de 65, os quais afirmam que sim e 21 não, o que corresponde a 75,58% e 24,42%, respectivamente.

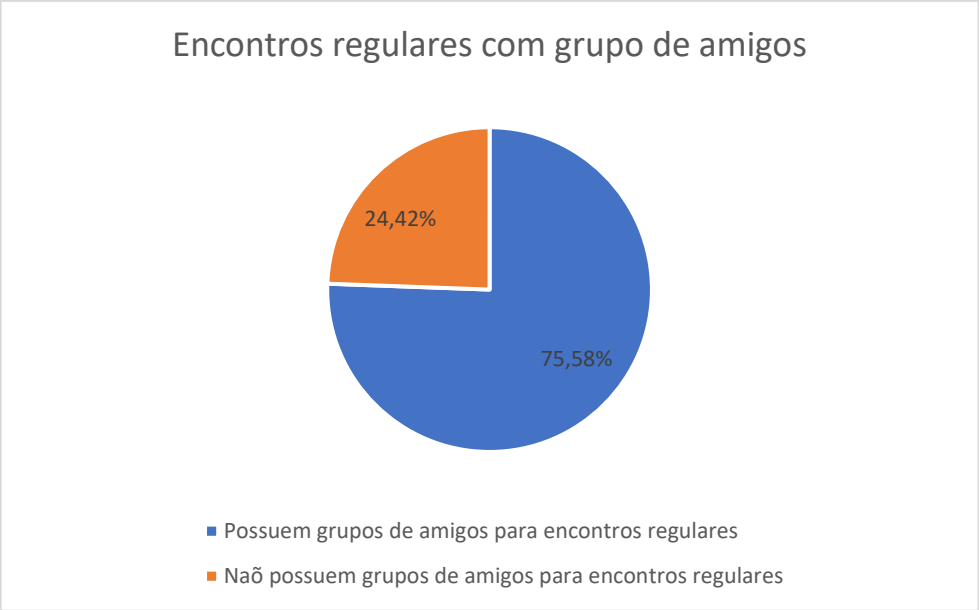


Gráfico 40 – Encontro físicos regulares de adolescente do sexo masculino

Com relação a frequentar ou não lugares além da escola, de forma regular, obtivemos os números de 62 que disseram sim, equivalendo a 72,09% e 24 disseram que não frequentam outros lugares, regularmente, sendo este equivalente a 27,91%.

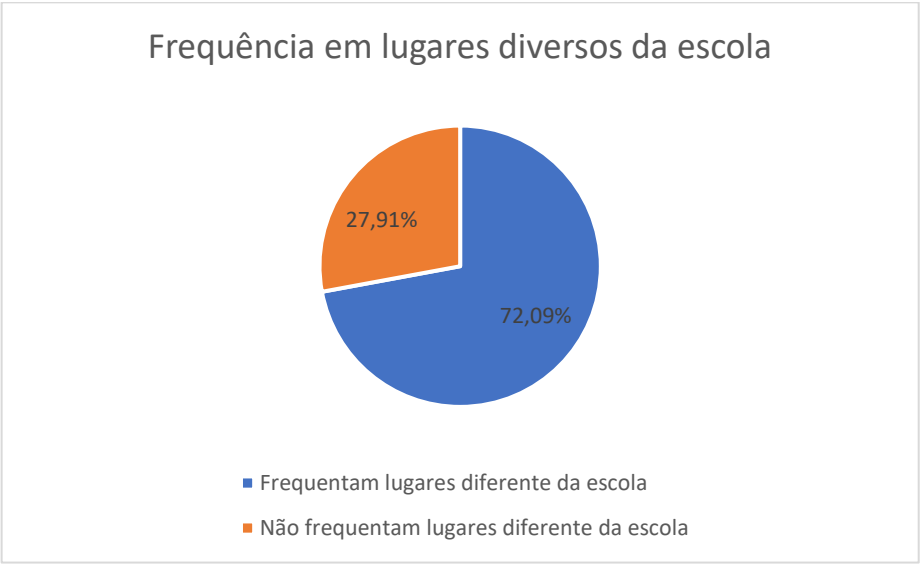


Gráfico 41 – Frequência em lugares diversos da escola de adolescente do sexo masculino

Ao cruzarmos os dados, observamos que 41 adolescentes masculinos têm atividade extraescolar, possuem grupos de amigos para encontros regulares e saem de casa para socializar em outros locais, fisicamente. Em percentual teremos o valor de 47,67%.

Por outro lado, tivemos 3 participantes masculinos os quais não possuem atividades extraescolares, nem possui amigos para encontros físicos e nem saem para lugares diferentes da escola para socializar. Isso corresponde a 3,48%.

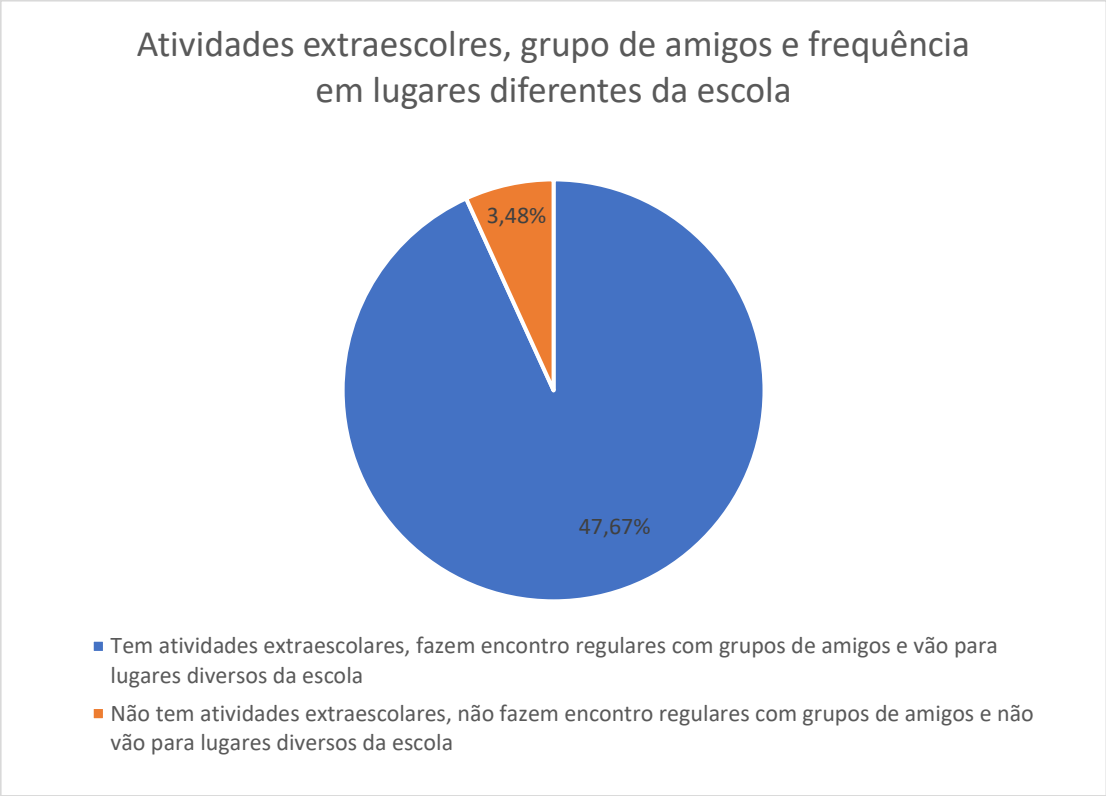


Gráfico 42 – Combinação entre atividades extraescolares, encontros físicos e lugares diversos da escola de adolescente do sexo masculino

8.4.5 – Análise de socialização dos adolescentes, do sexo feminino e masculino, com contato desconhecido pelo seu responsável e que saem para socializar

Verificamos que, 48 das adolescentes saem para socializar em locais diferentes do ambiente escolar, o que corresponde a 42,10%. Isso nos mostra um certo grau de perigo, já que sair para lugares com pessoas desconhecidas, podem fazer destes um alvo fácil para serem vítimas de um criminoso, o qual pode ter utilizado ferramentas digitais para fazer essa aproximação acontecer, valendo-se da Internet para marcar encontros em lugares, geralmente, favoráveis ao cometimento de delitos.

Por outro lado, em se tratando de adolescentes do sexo masculino, extraímos que 39 dos seus respectivos responsáveis não conhecem os contatos virtuais, o que implica em 45,34%. Todavia, estes saem para socializar em locais diferentes da escola.

Gráfico 43 – Combinação entre contatos desconhecidos e saída para socialização de adolescentes do sexo masculino e feminino

8.4.6 – Análise dos adolescentes, do sexo feminino e masculino, que usam o quarto para conectar à Internet, e possuem contatos desconhecidos pelo seu responsável e que saem para socializar

Esta análise, mostra um risco ainda maior, já que o adolescente usa Internet dentro do seu quarto, falando com pessoas desconhecidas de seus responsáveis e ainda sai para lugares extraescolares, com objetivo de socializar. Assim, obtivemos o número de 45 participantes do sexo feminino, o que representa 39,47%, e 39 do sexo masculino, que traz o percentual de 41,86%.

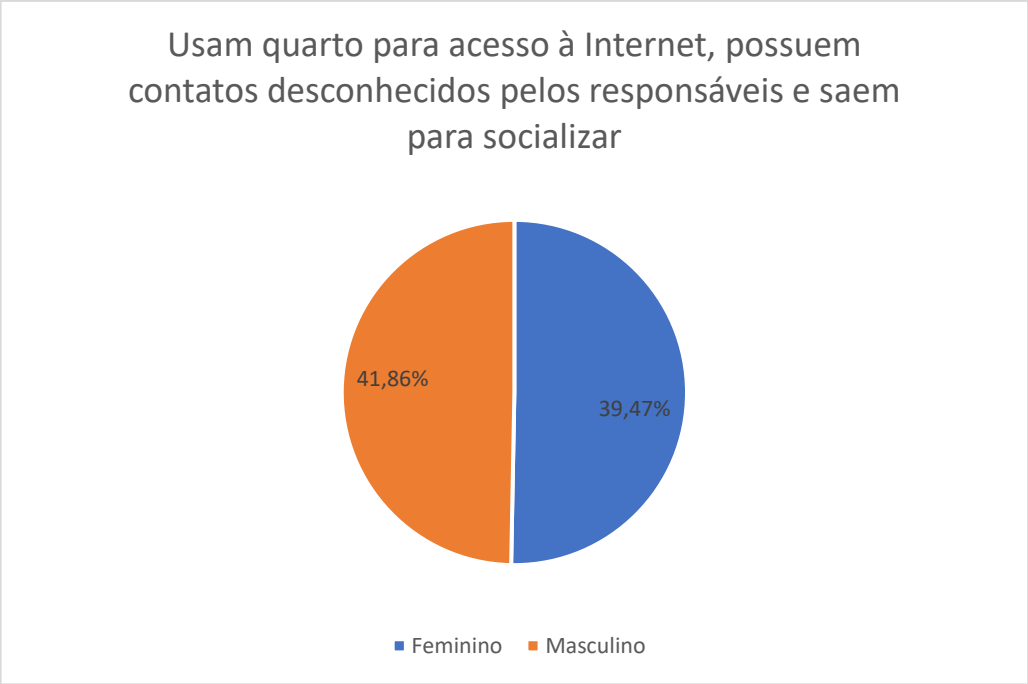


Gráfico 44 – Combinação entre acesso à Internet dentro do quarto, contatos desconhecidos e saída para socialização de adolescentes do sexo masculino e feminino

8.4.7 – Análise dos adolescentes, do sexo feminino e masculino, que usam o quarto para conectar à Internet, não são monitorados, possuem contatos desconhecidos pelo seu responsável e que saem para socializar

O risco ainda tem um aumento maior à medida que percebemos o quão livre os adolescentes ficam ao utilizarem as ferramentas e serviços conectados à Internet. A falta de monitoramento, somado com desconhecimento dos contatos pelos responsáveis, o acesso ao ciberespaço dentro do quarto e a saída para lugares além da escolar para socializar-se, nos mostra que é um cenário perfeito para ação de cibercriminosos que, ultrapassam as fronteiras do virtual e acabam por praticarem delitos no mundo real.

Após a filtragem destes dados, chegamos ao número de 20 participantes do sexo feminino e 16 do masculino, o que corresponde, respectivamente, em percentagem, a 17,54% e 18,60%.

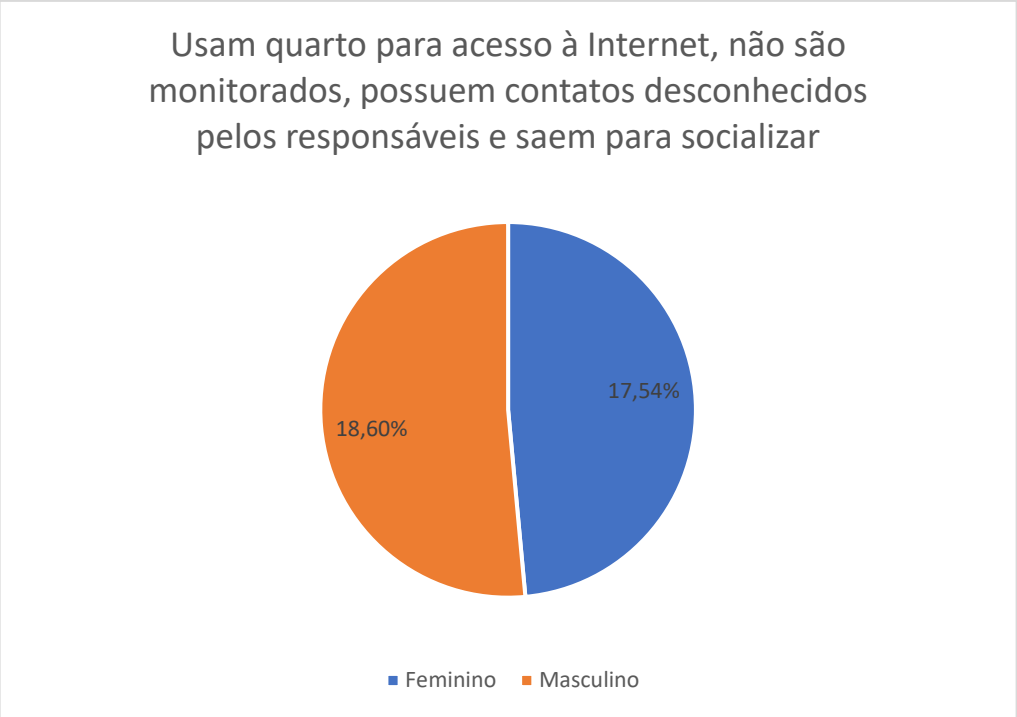


Gráfico 45 – Combinação entre acesso à Internet dentro do quarto, sem monitoramento, com contatos desconhecidos e saída para socialização de adolescentes do sexo masculino e feminino

8.4.8 – Análise dos adolescentes, do sexo feminino e masculino, que usam o quarto para conectar à Internet, não são monitorados, possuem contatos e publicações desconhecidas pelo seu responsável e saem para socializar

Neste conjunto de critérios, onde teremos, cada vez mais chances de traçarmos o perfil de uma vítima em potencial, detectamos que temos 13 adolescentes do sexo feminino e 5 do sexo masculino, os quais representam 11,40% e 5,81%, respectivamente.

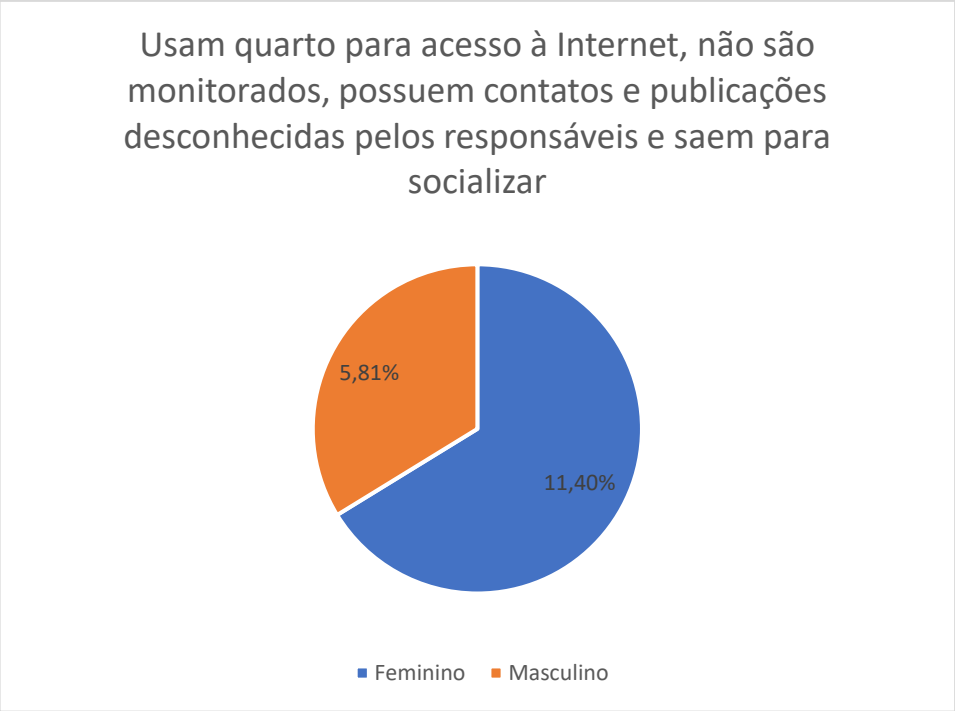


Gráfico 46 – Combinação entre acesso à Internet dentro do quarto, sem monitoramento, com contatos e publicações desconhecidas e saída para socialização de adolescentes do sexo masculino e feminino

Percebemos também que, nestes quesitos, os responsáveis pelas meninas são menos cuidadosos do que com os meninos. Aí nasce uma preocupação, tendo em vista que a incidência de crimes contra dignidade sexual é bem mais acentuada com mulheres.

8.4.9 – Análise dos adolescentes, do sexo feminino e masculino, que usam o quarto para conectar à Internet, não são monitorados, possuem contatos e publicações desconhecidas pelo seu responsável, saem para socializar e há um desconhecimento, por parte dos pais, do assunto cibercrimes

Na medida que temos um somatório dos questionamentos, os riscos de vitimização desses adolescentes irão subindo, e aqui identificamos os valores de 0 para sexo feminino e 1 para sexo masculino, o que traduzido em percentual seriam 0% e 1,16%.

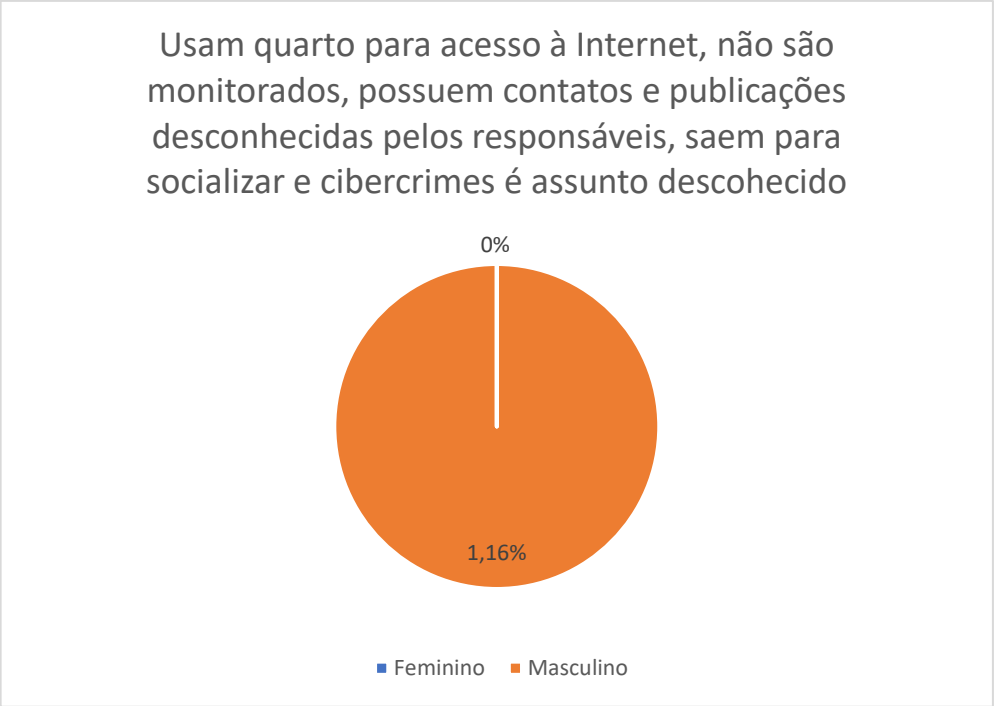


Gráfico 47 – Combinação entre acesso à Internet dentro do quarto, sem monitoramento, com contatos e publicações desconhecidas, são leigos no assunto cibercrimes e saída para socialização de adolescentes do sexo masculino e feminino

Notamos que, apesar de muito baixo o número de adolescentes que possuem tamanha vulnerabilidade. Nestes requisitos, o descuido com os meninos se mostrou maior.

8.4.10 – Análise dos adolescentes, do sexo feminino e masculino, que usam o quarto para conectar à Internet, não são monitorados, possuem contatos e as publicações desconhecidas pelo seu responsável, saem para socializar e há um desconhecimento, por parte dos pais, do assunto cibercrimes e da possível prática contra seu filho(a)

De forma progressiva, chegamos a um nível elevadíssimo de risco do adolescente ser vítima de um cibercriminoso, e neste obtivemos os resultados de 1 do sexo masculino e 1 do sexo feminino. 1,16% e 0,87%, respectivamente.

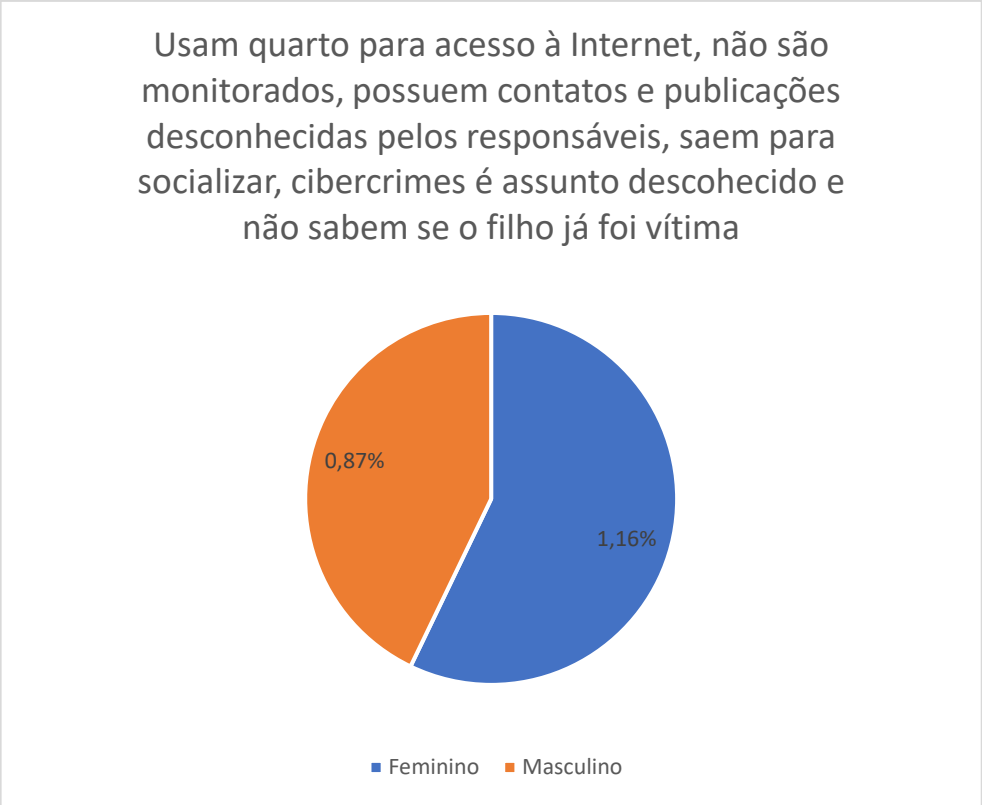


Gráfico 48 – Combinação entre acesso à Internet dentro do quarto, sem monitoramento, com contatos e publicações desconhecidas, são leigos no assunto cibercrimes, não sabem se o filho já foi vitimizado por cibercriminoso e saída para socialização de adolescentes do sexo masculino e feminino.

Levando em consideração o percentual, podemos afirmar que é muito baixo o número de adolescentes que estaria à mercê do cibercriminosos de maneira latente. Todavia, não podemos deixar de fazer uma análise levando em consideração que cada vida é de importância incalculável.

8.5 – Confrontar o manual

As perguntas 1 (Que idade tem o adolescente?) e 3 (Que ano/curso frequenta o adolescente?) do questionário aplicado, estão associadas aos seguintes quesitos e respostas da cartilha:

- Pergunta e resposta 14 (Qual a faixa etária que a lei considera adolescente?) da cartilha – Aqui mostraremos o que dispõe a lei brasileira denominada Estatuto da Criança e do Adolescente.
- Pergunta e resposta 15 (O que é uma pessoa vulnerável? Por que adolescente é considerado vulnerável à cibercrimes?) da cartilha – Esclarecemos o que é ser uma pessoa vulnerável, e ainda, mostraremos os motivos dos adolescentes serem considerados pessoas que se enquadram em tal conceito.
- Quesito e resposta 16 (Por que o adolescente é manipulado, facilmente, psicologicamente?) da cartilha – Percebermos aqui, o porquê a faixa etária que nos propomos a pesquisar possui características que os tornam de fácil manipulação.
- Quesito e resposta 17 (Quais as estratégias utilizadas para atrair os adolescentes?) da cartilha – Alertar sobre a maneira as quais os criminosos se utilizam para atrair as suas vítimas adolescentes.

A pergunta 4 (O adolescente possui acesso à dispositivos conectados à Internet (*smartphone*, *tablet*, computador etc.)?) do questionário aplicado, está ligada as seguintes perguntas e respostas:

- Pergunta e resposta 1 (O que é a Internet?) da cartilha – Neste aspecto iremos mostrar o conceito que, muitas vezes, passa desapercebido, isto é, as pessoas utilizam sem saber a dimensão que a rede mundial de computadores tem.
- Pergunta e resposta 2 (O que é Ciberespaço?) da cartilha – Após conhecer o conceito de Internet, importante saber o terreno o qual se navega, e para isso, mostraremos.
- Pergunta e resposta 3 (O que é *Surface Web*, *Deep Web* e *Dark Net*?) da cartilha – Aqui o leitor conhecerá o outro lado da Internet, qual seja, o lado sombrio onde são praticados muitos delitos. Além da dimensão e a sua relação com o acesso da Internet/Web.

- Pergunta e resposta 4 (O que são Cibercrimes?) da cartilha – Ensinar o conceito de cibercrimes para que o leitor possa estar familiarizado com as ramificações do assunto, que são introduzidas na cartilha.
- Pergunta e resposta 5 (O que é Cibersegurança?) da cartilha – Mostrar as formas de proteção contra os ataques cibernéticos.
- Pergunta e resposta 9 (O que são vírus de computadores e *malware*?) da cartilha – Conhecer as principais maneiras de se ser infectado por vírus ou *malware*, ajudará a identificar anormalidades causadas nos computadores e, assim, tomar providências para não se ser vítima dos cibercriminosos.

As perguntas 5 (O adolescente possui alguma rede social (*Facebook*, *Instagram*, *WhatsApp*, etc.)?), 7 (O responsável está ligado ou tem acesso às publicações nas redes sociais do adolescente?), 9 (O responsável faz o controle desse acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal?) e 10 (O responsável conhece todos os contatos virtuais do adolescente?) do questionário aplicado, estão justificadas nas seguintes orientações da cartilha:

- Pergunta e resposta 4 (O que são Cibercrimes?).
- Pergunta e resposta 5 (O que é Cibersegurança?).
- Pergunta e resposta 6 (O que é *Ciberbullying*?) – Importante identificar qualquer forma de *bullying* causado por meio da Internet, para que sejam tomadas as providências adequadas, inclusive, acionando os órgãos públicos competentes.
- Pergunta e resposta 7 (que é *Ciberstalking*?) – Reconhecer que está sendo vítima de perseguição, para que sejam tomadas as providências adequadas, inclusive, acionando os órgãos públicos competentes.
- Pergunta e resposta 8 (O que são *Fake News*?) – Saber a verdade sobre as notícias que ler, antes de acreditar ou até mesmo propagar.
- Pergunta e resposta 23 (Quais os males que as redes sociais podem trazer?) – Ter consciência dos prejuízos, em especial, psicológicos que as redes sociais podem trazer para a vida dos adolescentes.

A pergunta 11 (Quanto tempo em média o adolescente fica conectado à Internet?) do questionário aplicado, estar relacionadas a seguintes informações trazidas na cartilha:

- Pergunta e resposta 20 (Qual seria o tempo ideal de acesso para um adolescente?) – Aprender a controlar o tempo de uso de Internet é um fator que reduz muito os riscos de os adolescentes serem vítimas de cibercrimes.
- Pergunta e resposta 21 (Quais os males podem trazer o excesso de horas conectados à Internet?) – Reconhecer os sintomas de algumas doenças física e psicológicas, para então procurar ajuda de profissionais habilitados para o problema, sejam médicos ou psicólogos.

As perguntas 12 (O adolescente possui atividades extraescolares ou desporto, de forma frequente?), 13 (O adolescente possui um grupo de amigos regulares com quem se encontra fisicamente?) e 14 (O adolescente sai de casa de forma regular para ir a locais além da escola, para socializar?) do questionário aplicado, serviram como base para os seguintes informativos trazidos pela cartilha.

- Pergunta e resposta 6 (O que é *Ciberbullying*?).
- Pergunta e resposta 7 (que é *Ciberstalking*?).
- Pergunta e resposta 21 (Quais os males podem trazer o excesso de horas conectados à Internet?).
- Pergunta e resposta 22 (O que são desafios da Internet e quais os seus objetivos?) – Conhecer os perigos que esses desafios trazem para saúde física e psíquica dos adolescentes, bem como, identificar qualquer atitude suspeito as quais possam mostrar que seu filho (a) está participando de um desses desafios.
- Pergunta e resposta 23 (Quais os males que as redes sociais podem trazer?).
- Pergunta e resposta 26 (Como atuam os cibercriminosos?) – Detectar e se prevenir contra as formas utilizadas pelos cibercriminosos para concretizar os seus mais diversos ciberataques.
- Pergunta e resposta 27 (O que é capitalismo de vigilância virtual?) – Saber que tudo que se faz na Internet é compilado e, depois, utilizado para monitorar e influenciar as pessoas, de acordo com seus perfis.

- Pergunta e resposta 28 (Quais consequências psicológicas podem ter as vítimas de cibercrimes?) – Conhecer os diversos tipos de transtornos psicológicos que podem afetar seus filhos.

A pergunta 15 (O adolescente usa computadores ou *smartphone* no seu quarto?) do questionário aplicado, está ligada as seguintes questões trazidas pela cartilha:

- Pergunta e resposta 24 (O que são *nudes*? O que é *sextorsion*?) – Orientar os adolescentes, no sentido de mostrar os riscos que podem acarretar um simples envio de fotos sensuais, nudismo ou de cunho pornográfico.
- Pergunta e resposta 26 (Como atuam os cibercriminosos?).

As perguntas 16 (O responsável sabe o que é cibercrime?), 17 (O responsável tem conhecimento que o adolescente já foi vítima de algum cibercrime?) e 18 (O responsável sabe a que Delegacia de Polícia Civil Especializada a qual deve recorrer caso do adolescente seja vítima de cibercrimes?) do questionário aplicado, se relacionam aos seguintes quesitos da cartilha:

- Pergunta e resposta 29 (Qual delegacia de polícia especializada procurar em caso de cibercrimes?) – Saber onde fazer ocorrência policial é de suma importância para que possa procurar a delegacia competente para atuar nas investigações dos cibercrimes.
- Pergunta e resposta 30 (Quais os problemas sociais que podem acarretar a não comunicação dos cibercrimes?) – Entender o quanto as informações trazidas pela cartilha podem ajudar a ter uma sociedade mais informada e com o conhecimento para agir de maneira correta, tanto na prevenção quanto na repreensão.

As perguntas 19 (O responsável acha importante a divulgação sobre cibercrimes e cibersegurança nos meios de comunicações oficiais?), 20 (O responsável acha importante as escolas abordarem tema como o cibercrime e a cibersegurança?) e 21 (O responsável gostaria de ter acesso a uma cartilha de instruções que mostra os principais cibercrimes e o modo de prevenção, voltado, especialmente, aos adolescentes?) do questionário aplicado, estão diretamente ligadas às questões colocadas pela cartilha nas seguintes disposições:

- Pergunta e resposta da primeira até a última – Depois de todo conhecimento adquirido pelo conteúdo disposto na cartilha, é importante sabermos o interesse dos responsáveis sobre os temas cibercrimes e cibersegurança.

8.6 – Dados estatístico da cidade usada para o estudo

De acordo com anuário estatístico do município de Belém, o qual é a capital do Estado do Pará, obtivemos informações relacionadas com a população no ano de 2020, sendo este o mais recente, o qual aponta que a quantidade de pessoas com idade entre 10 e 14 anos é de 114.729, e entre 15 e 19 anos 121.284. Vale ressaltar que, nossa pesquisa se baseia na faixa etária de 12 a 17 anos, todavia, a divisão feito pelo site oficial da Secretaria Municipal de Planejamento não traz com exatidão tão faixa. Acrescentamos que, a população total do município de Belém é de 1.499.641 de habitantes.

Na tabela a seguir podemos visualizar a população, de cada faixa etária, do ano de 2011 até 2020.

SEGEP SECRETARIA MUNICIPAL DE PLANEJAMENTO — PREFEITURA DE BELÉM

DEMOGRAFIA

Tabela 13 - População Residente por Grupos de Idade, no Município de Belém - 2011 a 2020.

Faixa Etária	Ano									
	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
0 a 4 anos	110.335	108.744	107.312	104.104	102.086	88.979	87.107	85.912	84.462	82.848
5 a 9 anos	114.480	113.681	112.655	110.014	108.521	105.067	101.402	97.647	94.538	92.309
10 a 14 anos	117.705	117.813	117.964	116.285	116.034	117.102	117.018	116.759	116.066	114.729
15 a 19 anos	124.778	123.205	121.851	123.362	123.255	125.129	124.343	123.302	122.279	121.284
20 a 29 anos	269.304	263.066	256.485	250.015	244.055	249.831	247.105	244.478	241.658	238.451
30 a 39 anos	236.991	240.752	244.219	244.969	246.258	256.168	256.398	255.988	255.060	253.682
40 a 49 anos	183.483	187.028	190.654	193.622	197.434	208.970	213.239	217.622	222.212	227.034
50 a 59 anos	130.081	134.440	138.610	142.148	146.348	152.920	156.937	161.154	165.562	170.154
60 a 69 anos	72.154	75.625	79.304	83.771	88.372	96.366	100.838	105.442	110.052	114.591
70 a 79 anos	36.799	38.364	40.013	41.403	43.082	48.880	51.078	53.346	55.758	58.381
80 anos e mais	15.362	16.085	16.855	17.675	18.536	22.259	23.136	24.082	25.098	26.178
Total	**1.411.472**	**1.418.803**	**1.425.922**	**1.427.368**	**1.433.981**	**1.471.671**	**1.478.601**	**1.485.732**	**1.492.745**	**1.499.641**

Fonte: 2000 a 2013 - Estimativas preliminares efetuadas em estudo patrocinado pela Rede Interagencial de Informações para a Saúde - Ripsa.
2014 e 2015 – Estimativas preliminares elaboradas pelo Ministério da Saúde/SVS/CGIAE.
2016 a 2020 - DATASUS

Figura 38 – População do município de Belém por faixa etária

A nossa pesquisa contou com 200 participantes, isto é, se pegarmos uma média da população do somatório das faixas de 10 a 14 e de 15 a 19 anos, isto é, o valor de 114.729 somando com 121.284 será igual a 236.013 e, logo em seguida, dividirmos por 10, o que representam as idades de 10, 11, 12, 13, 14, 15, 16, 17, 18 e 19, obteremos o resultado de 23.601, e depois multiplicarmos pelo número de 6, o qual representam as idades de 12, 13, 14,

15, 16 e 17 anos, chegaremos ao valor populacional dessa faixa etária de 141.606 adolescentes, aproximadamente, de ambos os sexos. Vale ressaltar que, nossa entrevista por meio de formulário, se deu com 0,141% da população total de adolescentes, em média.

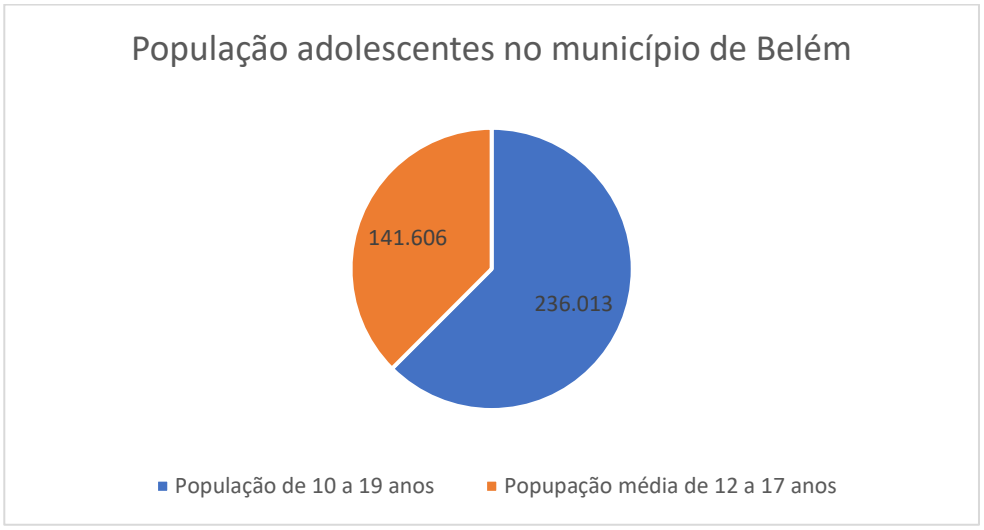


Gráfico 49 – População adolescentes no município de Belém do Pará

Quando pegamos o número total da população e comparamos com a média de adolescentes as quais extraímos anteriormente, obtivemos que 9,442 % é constituída de adolescentes (12 a 17 anos).

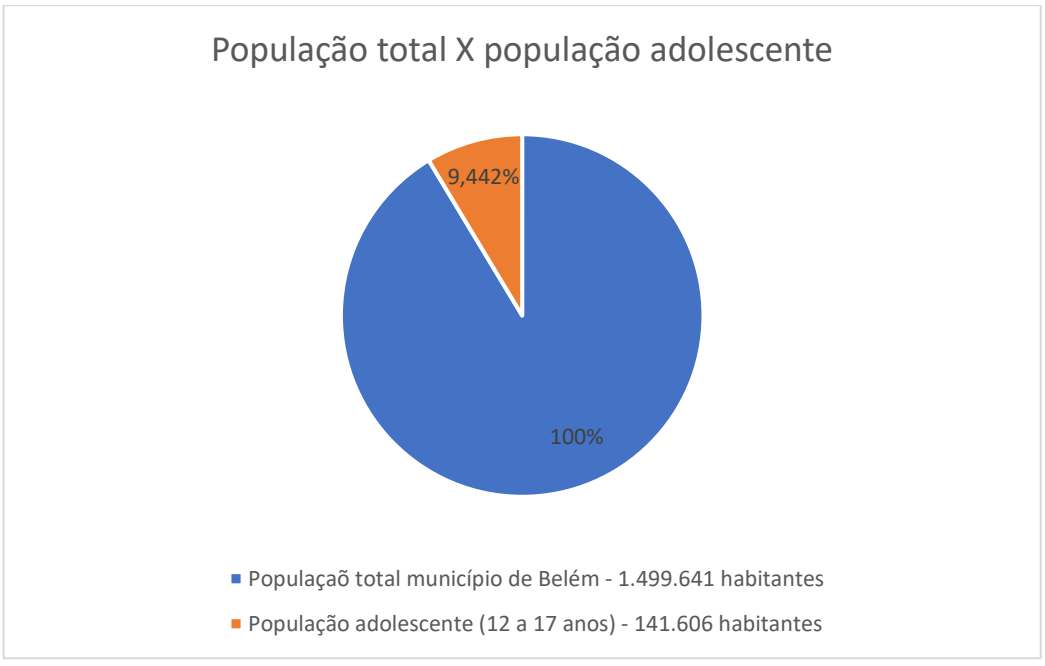


Gráfico 50 – População total versus população de adolescentes do município de Belém.

8.7 – Estratégia do governo brasileiro relacionado a segurança da informação

O governo brasileiro criou o decreto nº 9.637, de 26 de dezembro de 2018, para instituir a Política Nacional de Segurança da Informação (Brasil, 2018) e, assim tratar do tema cibersegurança, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional.

Neste contexto, o decreto procura abranger a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais e as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Dentre os vários princípios assegurados por este decreto, temos o respeito as garantias fundamentais trazidas pela Constituição Federal, qual seja, a liberdade de expressão que abrange a proteção de dados pessoais, a privacidade e o acesso à informação. Vale ressaltar, a preocupação em fomentar a cultura em segurança da informação e, ainda, a integração e cooperação entre o Poder Público, o setor empresarial, a sociedade e as instituições acadêmicas.

O artigo 4º do decreto nº 9.637, traz os seguintes objetivos:

> Art. 4º São objetivos da PNSI:
> I – contribuir para a segurança do indivíduo, da sociedade e do Estado, por meio da orientação das ações de segurança da informação, observados os direitos e as garantias fundamentais;
> II – fomentar as atividades de pesquisa científica, de desenvolvimento tecnológico e de inovação relacionadas à segurança da informação;
> III – aprimorar continuamente o arcabouço legal e normativo relacionado à segurança da informação;
> IV – fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação;
> V – fortalecer a cultura da segurança da informação na sociedade;
> VI – orientar ações relacionadas a:
> a) segurança dos dados custodiados por entidades públicas;
> b) segurança da informação das infraestruturas críticas;
> c) proteção das informações das pessoas físicas que possam ter sua segurança ou a segurança das suas atividades afetada, observada a legislação específica; e
> d) tratamento das informações com restrição de acesso; e
> VII – contribuir para a preservação da memória cultural brasileira.

Ainda temos o decreto nº 10.748, de 16 de julho de 2021, e que Institui a Rede Federal de Gestão de Incidentes Cibernéticos (Brasil, 2021), o qual trata da colaboração entre os órgãos da administração direta e indireta, bem como de empresas públicas e das sociedades de economia mista federal, tendo seus objetivos trazido pelo artigo 3º, que mencionam:

> Art. 3º São objetivos da Rede Federal de Gestão de Incidentes Cibernéticos:
> I – divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos;
> II – compartilhar alertas sobre ameaças e vulnerabilidades cibernéticas;
> III – divulgar informações sobre ataques cibernéticos;
> IV – promover a cooperação entre os participantes da Rede; e
> V – promover a celeridade na resposta a incidentes cibernéticos.

Diante o exposto, verificamos que há uma preocupação do governo em trata do tão importante tema de cibercrimes, todavia, percebemos uma forma de prevenção geral, porém, a proteção de forma específica dos adolescentes, os quais tratamos como vulneráveis, ainda não foi implementado nenhuma proposta pelo governo. Vale ressaltar que, essa especificidade de proteção relacionada com a cibersegurança dos adolescentes é o foco principal deste trabalho, mostrando o quanto será útil para a sociedade, já que estamos tratando de um tema de relevância mundial e de que pouco se tem material sobre este tema específico.

8.8 – Sensibilidade por parte do governo do município de Belém do Pará em comparação ao de Portugal

Em muitos países, como Portugal, existem ações presenciais e *online*, bem como um conjunto de ações que visam sensibilizar a integradas nas atividades curriculares e extracurriculares do ensino fundamentais e médios e, que têm como alcance potencial todo o universo escolar, já que o tema é de interesse geral.

No município de Belém, no Estado do Pará, não há ações relacionadas com a divulgação de prevenção contra cibercrimes. Não existe assim, nenhum plano de governo voltado para a elaboração de ações que tenham por objetivo propagar o tema relacionado com a cibersegurança, em especial, para a população específica dos adolescentes, pois, como visto,

estão em fases evolutiva da vida, o que os tornam mais vulneráveis a serem vítimas em potencial dos cibercriminosos.

Percebemos, também, que em Portugal as ações voltadas para divulgação de cibersegurança, na sua maioria, são voluntárias. Podemos inferir que, tal país vem tendo um crescente aumento nos cursos que se dedicam ao tema cibersegurança, incluindo até graduação de nível superior nesta área. Por outro lado, apesar de existirem cursos sobre o tema, estes, no Brasil, são explorados por profissionais da área TI, os quais não tem interesse de propagar as informações para um público geral, deixando, assim, cada vez mais distante o contato entre o tema e a sociedade como um todo.

8.9 – Dados de Portugal sobre o acesso à Internet dos adolescentes

Para confirmar o nosso entendimento em relação ao comportamento das pessoas, em especial os adolescentes, foram recuperados dados oficiais relacionados com o acesso à Internet (INEP, 2019), procurando informação geral sobre a conectividade dos usuários à rede mundial de computadores.

Em 2019, verifica-se que mais 80% dos agregados familiares têm acesso à Internet em Portugal, e este acesso ser em banda larga; verifica-se mesmo que o maior percentual de acesso está nas famílias com crianças até 15 anos. Em complemento, a maior utilização da Internet/Web é realizado por pessoas que completaram o nível superior (98,7%), seguido pelos que concluíram o secundário (96,9%). Vale ressaltar que, o acesso à Internet/Web é maior entre o público mais jovem, isto é, pessoas de mais idade têm menor contato com a Internet/Web.

Ano: 2019	Unidade: %
Total	**76,2**
Sexo	
Homens	77,5
Mulheres	75,0
Escalões etários	
16 a 24 anos	99,5
25 a 34 anos	98,2
35 a 44 anos	95,2
45 a 54 anos	79,6
55 a 64 anos	59,3
65 a 74 anos	34,1
Nível de escolaridade completo	
Até ao básico - 3.º ciclo	55,6
Ensino secundário	96,9
Ensino superior	98,7

Figura 39 – Acesso à Internet por faixa etária e escolaridade em Portugal

Quando se considera o acesso à Internet/Web em mobilidade, verifica-se que 84,1% utilizam equipamento portáteis, principalmente *smartphones*, e que a cada ano, vem aumentando de forma significativa o peso deste tipo de acesso, conforme mostram os gráficos a seguir.

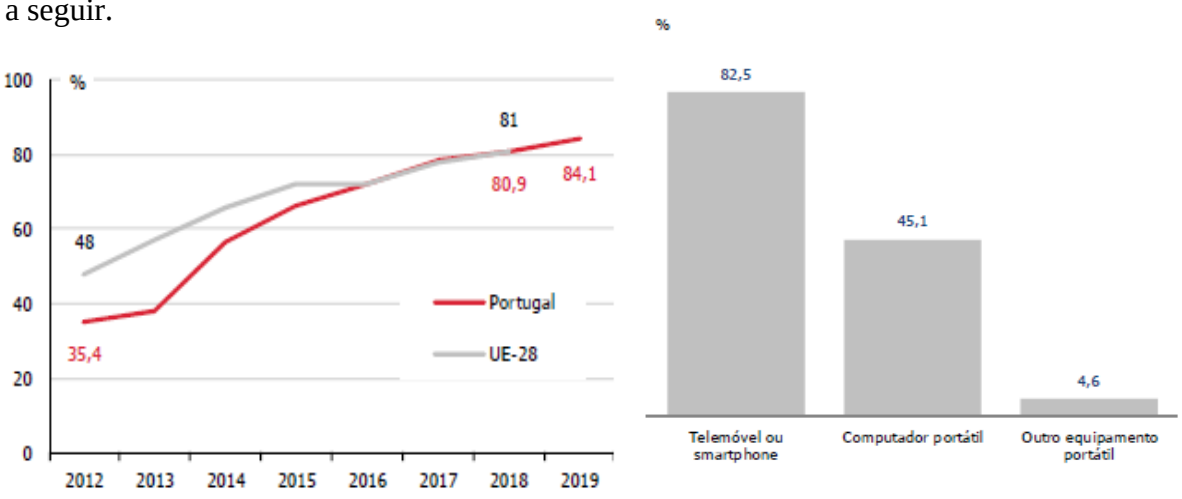


Figura 40 – Gráfico de acesso por meio de dispositivos móveis em Portugal

Em complemento, 80% dos utilizadores da Internet/Web participam de redes sociais e, esta tendência vem aumentando a cada dia. Por outro lado, temos uma redução de pessoas que utilizam a Internet/Web para manter contato com algum órgão da administração pública.

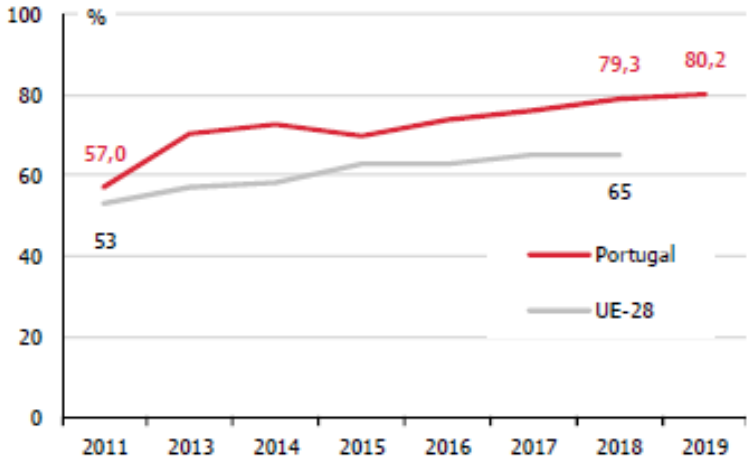


Figura 41 – Acesso a redes sociais em Portugal

A Internet/Web oferece diversos serviços que podem ser utilizados dependendo do propósito do usuário e, em Portugal essa utilização ficou distribuída da seguinte forma, como mostra a figura a seguir.

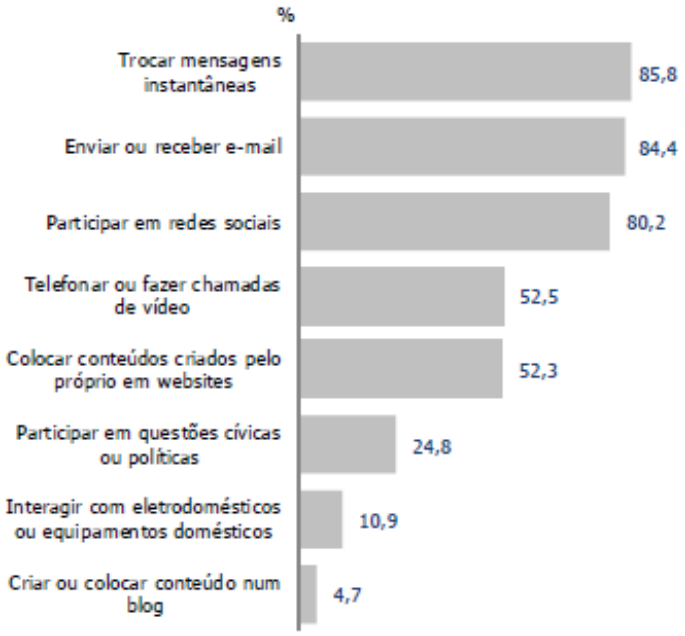


Figura 42 – Utilização de serviços na Internet em Portugal

Em uma pesquisa realizada no ano de 2021 pela Yskills é apresentado, de uma população com faixa etária entre 12 e 17 anos, dados relativos à sua distribuição socioeconômica (Pontes & Batista & Baptista, 2022): 1% possui dificuldade; 41% vivem mais ou menos; 50% vivem bem e 8% vivem muito bem, como mostra a figura a seguir.

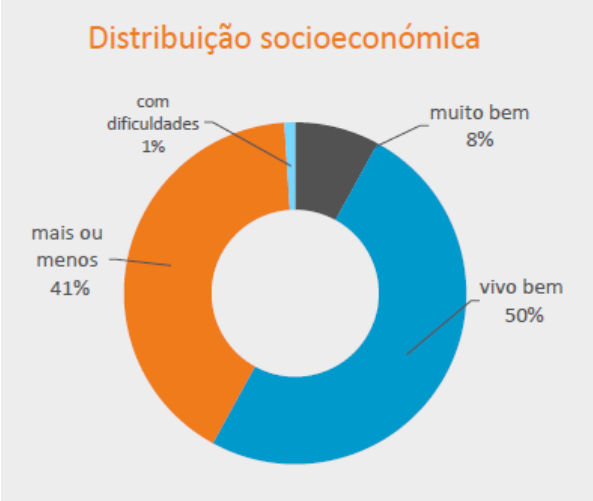


Figura 43 – Distribuição socioeconômica dos adolescentes de Portugal

Ao considerarmos a proporção de competência digital dos entrevistados, obtivemos os seguintes dados.

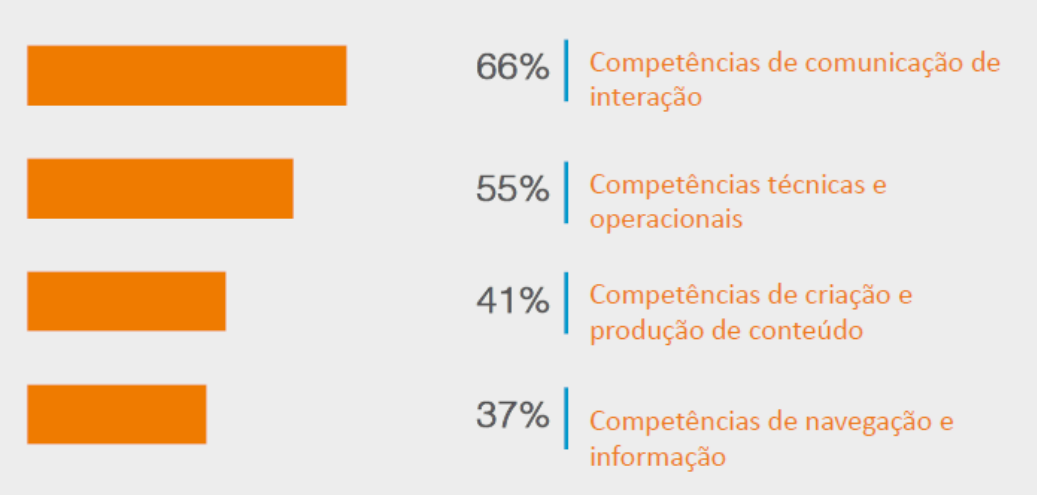


Figura 44 – Competências digitais em Portugal

Assim, uma percentagem de 45% de adolescentes, do sexo masculino e feminino, possuem conhecimento do digital e, este aumenta com a idade. É possível afirmar que, o desenvolvimento mental dos adolescentes tendem a fazer com que estes tenham mais maturidade e se tornem cada vez menos vulneráveis em relação a ataques de cibercriminosos.

Diversos autores demostram que desde a criação de redes sociais, estas passaram a ser a preferencia de entretenimento dos adolescentes. Em especial, as meninas internalizam mais os contatos e o suporte social e emocional, o que pode vir a ser um fator gerador de um potencial problema psicológico, enquanto os meninos externalizam essas questões e tendem a gerar conflitos, aumentando os casos de violência.

Relembrando a prevenção como o foco de nosso estudo, verificamos que são várias as pesquisas que mostram que a família e a escola desempenham um papel fundamental na preparação do comportamento do adolescente diante do seu acesso ao ciberespaço, visto que é de extrema relevância que os usuários mais jovens sejam orientados e a eles sejam mostrados os riscos reais que podem ter de enfrentar.

Por outro lado, não se deve proibir o acesso à Internet, já que esta se tornou uma fonte inesgotável de conteúdo. A Internet deve ser utilizada como uma forma complementar para o enriquecimento de tarefas e de trabalhos escolares e, deve ser utilizada de maneira exploratória, pois é essencial no contexto extraescolar. A sua importância e, em especial, das plataformas digitais é indiscutivel na nossa sociedade.

Em consequência, podemos inferir que, é da maior importância essa interatividade dos adolescentes com a rede mundial de computadores. Porém, o monitoramento por parte dos pais ou responsáveis legais devem ser prioridade, com o objetivo de reduzir os riscos de estes serem vitimizados por cibercriminosos. Além disso, é importante envolver os adolescentes na identificação dos problemas causados pelo uso excessivo da tecnologia, em especial, as associadas à Internet/Web, fomentando, também, a prática de atividades sem conexões (Matos et al., 2019).

8.10 – Resumo do capítulo

Neste capítulo foram apresentadas as análises relacionadas com os grupos de questões do questionário realizado: identificação, conectividade, caracterização, hábitos e consciência, onde de cada um foram extraídos dados relevantes e importantes para se obter uma avaliação do potencial da cartilha realizada. Por exemplo, foi verificado o quão desregrado e perigoso chega ser o acesso à Internet/Web realizado pelos adolescentes.

No grupo 1, identificação, trouxemos um quadro mostrando a idade, a quantidade de adolescentes em cada idade e o seu grau de instrução. Na conectividade, obtivemos o valor de 100% de adolescente com acesso à Internet, onde 94,5% possuem acesso a redes sociais e 64% acessam às redes sociais dos seus responsáveis legais.

Os dados trazidos pelo grupo 3, caracterização, proporcionaram valores de 15% de responsáveis que possuem o nível fundamental de instrução escolar e em que 93,87% dizem saber o que os filhos publicam. Por sua vez, 87,09% fazem um controle de acesso e 80,64% conhecem os contatos virtuais dos adolescentes. Em relação aos responsáveis com nível médio de ensino temos 37%, dos quais 75,67% conhecem as publicações, 62,16% controlam o acesso e 31,08% conhecem os contatos. Finalmente, temos que 47,5% dos responsáveis possuem nível superior, e que destes 82,10% têm conhecimento das publicações e, 72,63% fazem algum tipo de controle de acesso, e, por último, 26,31% conhecem os contatos virtuais de seus adolescentes. Curioso verificar que, quanto maior o nível de instrução dos responsáveis, mais relaxado parece ser o controle exercido aos adolescentes, ainda que essa diferença seja ligeira.

Ao considerar o grupo 4, Hábitos, obtemos os seguintes valores: 24% dos adolescentes não fazem encontros com amigos de forma regular; 31% não saem de casa para lugares diversos da escola; e 86,5% utilizam os dispositivos conectados à Internet dentro do quarto. Talvez o conjunto de dados que lance maior alerta, por via de o podermos considerar hábitos de risco.

Finalmente, o grupo 5, consciência, informa que 70,5% dos responsáveis afirmam conhecer o conceito de cibercrime, porém, não tem conhecimento de que o filho foi ou não vítima de algum desses delitos. Verifica-se, igualmente, com 92%, uma aceitação da cartilha proposta neste trabalho.

Em seguida foi partilhado um quadro de resumo dos grupos de questões e, então, partimos para as diversas combinações de dados, onde consideramos as conclusões dos diferentes grupos de questões e, se analisou o crescente risco em que alguns adolescentes incorrem ao desfrutar do ciberespaço sem quase nenhuma prevenção para combater a incidência de possíveis cibercrimes.

Após demonstrar atrávés dos dados, estes foram confrontados com os quesitos trazidos pelo questionário aplicado e a estrutura de pergunta e de respostas trazidas pela cartilha de prevenção proposta. Assim, justificaremos o porquê é importante incluir aquelas questões em específico.

As questões trazidas pelo questionário aplicado aos responsáveis pelos adolescentes foram: Que idade tem o adolescente?; Qual o gênero do adolescente?; Que ano/curso frequenta o adolescente?; O adolescente possui acesso à dispositivos conectados à Internet (*smartphone*,

tablet, computador etc.)?; O adolescente possui alguma rede social (*Facebook*, *Instagram*, *WhatsApp* etc.)?; O adolescente possui acesso às suas contas em rede social?; O responsável está ligado ou tem acesso às publicações nas redes sociais do adolescente?; Qual a escolaridade do responsável?; O responsável faz o controle desse acesso à Internet, seja por meio de programas específicos de segurança ou monitoramento pessoal?; O responsável conhece todos os contatos virtuais do adolescente?; Quanto tempo em média o adolescente fica conectado à Internet?; O adolescente possui atividades extraescolares ou desporto, de forma frequente?; O adolescente possui um grupo de amigos regulares com quem se encontra fisicamente?; O adolescente sai de casa de forma regular para ir a locais além da escola, para socializar?; O adolescente usa computadores ou *smartphone* no seu quarto?; O responsável sabe o que é cibercrime?; O responsável tem conhecimento que o adolescente já foi vítima de algum cibercrime?; O responsável sabe a que Delegacia de Polícia Civil Especializada a qual deve recorrer caso do adolescente seja vítima de cibercrimes?; O responsável acha importante a divulgação sobre cibercrimes e cibersegurança nos meios de comunicações oficiais?; O responsável acha importante as escolas abordarem tema como o cibercrime e a cibersegurança?; O responsável gostaria de ter acesso a uma cartilha de instruções que mostra os principais cibercrimes e o modo de prevenção, voltado, especialmente, aos adolescentes?.

As perguntas e respostas trazidas pela cartilha foram relacionadas aos conhecimentos a seguir: O que é a Internet?; O que é Ciberespaço?; O que é *Surface Web, Deep Web e Dark Net*?; O que são Cibercrimes?; O que é Cibersegurança?; O que é *Ciberbullying*?; O que é *Ciberstalking*?; O que são *Fake News*?; O que são vírus de computadores e *malwares*?; Quais programas podem ser utilizados para proteção de alguns cibercrimes? Quais comportamentos podem ser adotados para evitar os cibercrimes?; O que são comunidades virtuais?; O que são redes sociais? Quais seus objetivos?; Qual a faixa etária que a lei considera adolescente?; O que é uma pessoa vulnerável? Por que adolescente é considerado vulnerável à cibercrimes?; Por que o adolescente é manipulado, facilmente, psicologicamente?; Quais as estratégias utilizadas para atrair os adolescentes?; O que o Estatuto da Criança e do Adolescente traz sobre crimes praticados pela Internet?; O adolescente pode praticar atos criminosos pela Internet?; Qual seria o tempo ideal de acesso para um adolescente?; Quais os males podem trazer o excesso de horas conectados à Internet?; O que são desafios da Internet e quais seus objetivos? Quais os males que as redes sociais podem trazer?; O que são *nudes*? O que é *sextorsion*?; Quais os principais delitos que podem passar do campo virtual para o real?; Como atuam os cibercriminosos?; O que é capitalismo de vigilância virtual?; Quais consequências psicológicas podem ter as vítimas

de cibercrimes?; Qual delegacia de polícia especializada procurar em caso de cibercrimes?; Quais os problemas sociais que podem acarretar a não comunicação dos cibercrimes?.

Foram ainda mostrados dados estatísticos relacionados com o município em que a pesquisa foi realizada: os seus habitantes são 1.499.641, com uma população entre 10 e 14 anos e 15 e 19 anos, estimando uma média para mostrar o valor aproximado de adolescentes entre 12 e 17 anos, o foco principal do trabalho, e chegamos a 141.606 adolescentes.

Foi apresentado o decreto nº 9.637, de 26 de dezembro de 2018, que trata da Política Nacional de Segurança da Informação, bem como, as suas abrangências, o que pretende assegurar e os seus objetivos. Em seguida mostramos a sensibilidade do governo do município de Belém e, as suas intenções que visam realizar ações de divulgação do tema relacionado com a cibersegurança, embora tenhamos concluído que esta não é feita. Tal indicia o desinteresse, por parte dos governantes, na discussão e propagação de um tema tão atual e relevante para a nossa sociedade e para a proteção dos nossos jovens.

Foram exibidos dados estatísticos relacionados com a população do município de Belém, os quais mostraram que a quantidade de pessoas com idade entre 10 e 14 anos é de 114.729, e entre 15 e 19 anos 121.284, bem como a população total que é de 1.499.641 habitantes. Foi estimada uma população com valor aproximado de 141.606 na faixa etária de 12 a 17 anos.

Ao passarmos para as políticas utilizadas pelo governo brasileiro com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional, verificamos que foi criado o decreto nº 9.637, de 26 de dezembro de 2018, bem como, o decreto nº 10.748, de 16 de julho de 2021, o qual institui a Rede Federal de Gestão de Incidentes Cibernéticos.

Apresentamos a sensibilidade por parte do governo do município de Belém do Pará em comparação ao de Portugal e, verificamos que não há nenhuma política voltada para a divulgação de prevenção contra cibercrimes, diferentemente de Portugal onde existem, inclusive, a participação de voluntários para tal intento.

Passamos a mostrar os dados de Portugal em relação ao acesso à Internet dos adolescentes, e verificamos, que de facto, o comportamento em relação à era digital é semelhante à realidade mostrada no estudo feito no município de Belém. Vale a pena ressaltar que, os *smartphones* são os dispositivos responsáveis pela maior conectividade e as redes

sociais são as favoritas dos adolescentes que parece constituir assim, as suas forma principais de entretenimento. Deste modo, podemos dizer que a contribuição deste trabalho parece poder ser universalizada, pois o modo pelos quais os adolescentes se expõem na rede mundial de computadores, se assemelha no mundo inteiro.

Inferimos, finalmente, que, esta análise do cruzamento de dados dos diversos grupos, seja de forma individual ou entre grupos diferentes, possui alto grau de importância, tendo em vista esta forma de comunicação de cibercrimes e o quanto a proposta de uma cartilha para prevenção e cibersegurança pode contribuir para a sociedade, de forma a prevenir que os adolescentes sejam vítimas de cibercriminosos, passando a conscientizar o quão é importante acessar à Internet/Web de forma segura.

CAPÍTULO 9

Conclusão, obstáculos e trabalho futuro

9.1 – Introdução

Ao chegarmos ao último capítulo deste trabalho, apresentamos quais foram os resultados obtidos cujo maior objetivo foi o de aprofundar uma temática tão relevante que é a cibersegurança, envolvendo adolescentes. Assim, podemos afirmar o quão satisfatório foi percorrer por tantas fontes de conhecimento científico utilizadas para proporcionar a base para construção da cartilha de prevenção e cibersegurança para adolescentes e para os seus responsáveis.

Foi importante fazer uma revisão dos objetivos propostos no início da jornada e, verificamos que os objetivos geral e específicos foram concretizados. Também foi conseguido o cumprimento do cronograma estabelecido de forma metódica e buscando sempre informação coerente e relevante para informar o contributo do trabalho.

Além da preocupação com o cumprimento de todos os requisitos formais para a construção do trabalho, tivemos a sensibilidade de trazer algo que, de facto, irá contribuir, de forma positiva, para a sociedade e, em especial, para os pais e responsáveis por adolescentes que assim poderão desfrutar do resultado do trabalho para melhor orientar e, até mesmo, prevenir que os seus tutelados sejam vitimizados por cibercriminosos.

Finalmente, lançamos o desafio para futuros trabalhos, os quais podem complementar a cartilha de prevenção proposta, criando algo mais amplo, isto é, um manual de instruções relacionado com a resposta e a contingência a ataques de cibercrimes e a verificação de dispositivos de cibersegurança, já que o tema é inesgotável e de relevância mundial. No contexto do mundo contemporâneo e, até mesmo, no futuro, a tecnologia tende a evoluir e, assim, aumentar a dependência no uso dessas ferramentas, seja para atividades pessoais ou profissionais, seja pela própria evolução e sofisticação do mundos e dos dispositivos digitais.

9.2 – Revisando os objetivos do trabalho

O objetivo deste trabalho de investigação consistiu na apresentação de uma proposta para a comunicação de cibersegurança para o adolescente, com finalidade de reduzir a vitimização desses vulneráveis frente aos cibercriminosos.

Em um primeiro momento, começamos a envolver o pesquisador, trabalhando com a criação de artigos científicos que complemento este trabalho e que foram objeto de publicação (conforme partilha em apêndice). O percurso realizado permitiu mostrar o quão desinformados estão os pais ou responsáveis legais quando se trata de orientação e monitoramento de acesso à Internet/Web.

Em seguida, tínhamos como tarefa, a de demonstrar o quanto o assunto de cibersegurança era desconhecido, para isso, foi aplicado um questionário de 21 perguntas que permitiu a recolha de dados em planilhas para que fosse possível realizar uma análise e tirarmos as nossas conclusões.

Posteriormente, após a análise minuciosa e fazendo diversas combinações de dados, chegamos a conclusões, em especial, a que seria bem aceite a apresentação e divulgação de uma cartilha que pudesse informar e orientar as pessoas sobre os males da Internet/Web e o como e porquê dar importância ao conhecimento de técnicas de cibersegurança.

O quadro a seguir mostra o resumo dos objetivos do trabalho e, apresenta a maneira como, em nosso entender, foram alcançados, bem como observações complementares que julgamos importantes. Vale ressaltar que, o quadro é também uma forma de apresentar as etapas que foram realizadas para se chegar até à parte final e assim cumprir com aquilo que nos propusemos quando da apresentação do projeto de pesquisa.

Objetivos	Forma de cumprimento	Observações
1– Conhecer mais sobre o tema de cibercrimes e cibersegurança.	Pesquisas e leituras de diversos artigos científicos sobre o tema.	A colheita do conteúdo se deu em fontes oficiais, e com artigos publicados.
2 – Produzir artigos científicos para publicação.	Com base no conteúdo pesquisado e estudado, foram produzidos artigos.	Os artigos foram publicados no *International Journal of Advanced Engineering Research and Science* (IJAERS).
3 – Criação e aplicação de formulário para colher dados, dos pais e responsáveis legais, relacionados com o conhecimento sobre cibersegurança.	Os formulários foram aplicados por meio da plataforma *Google Forms* e, alguns, foram impressos e preenchidos manualmente pelos pais e responsáveis legais.	A aplicação se deu com pessoas de diversos níveis de formação educacional e classes sociais.
4 – Organização e análise dos dados colhidos.	Os dados foram colocados em planilhas do MS Excel e foram filtradas combinações para melhor tirar conclusões.	Relacionamos os dados respeitando a coerência da informação, para chegarmos em conclusões concretas.
5 – Criação da cartilha de prevenção.	Com base nas perguntas feitas no formulário, produzimos o conteúdo da cartilha.	Fizemos a análise de carência de conhecimento por parte dos pais, e então, colocamos em forma de perguntas e respostas na cartilha.
6 – Conclusão do trabalho.	Procuramos mostrar que todo o percurso realizado trará uma contribuição relevante para a sociedade.	Esperamos propagar, através de vários meios, o conteúdo dessa cartilha, para atingirmos o maior número de pessoas possíveis.

Tabela 34 – Objetivos, justificação de realização e observações

De modo geral, podemos afirmar que, o objetivo principal deste trabalho de investigação foi atingido, também por via, desde o início, de uma perfeita interação entre o pesquisador, o orientador e a própria pesquisa, fazendo com que todo o conteúdo fosse produzido de maneira sistemática e respeitando todas as normas estabelecidas para a produção do trabalho, envolvendo um significativo esforço e dedicação.

9.3 – Resultados obtidos

Após a realização da pesquisa científica podemos dizer que os resultados obtidos foram:

- Pesquisa satisfatória e de conteúdo científico, confiável para suportar o trabalho realizado;
- Recolha de dados envolvendo um número de respondentes que permitiu a obtenção de 200 respostas válidas, com pessoas disponíveis e interessadas em participar;
- Filtragem de dados para o perfeito enquadramento da pesquisa;
- Análise estatística feita dentro dos parâmetros de coerência e relevância;
- Conhecimento necessário para produzir a cartilha de prevenção contra cibercrimes;
- Produção e publicação de artigos científicos com temas atuais e de grande relevância para a nossa sociedade;
- Junção de informação com valor para pais e responsáveis, como por exemplo, as características dos adolescentes e a sua discussão no âmbito do tema em estudo – cibersegurança e cibercrimes;
- Grande aceitação por partes dos interessados: pais e responsáveis legais dos adolescentes;
- Incentivo para trabalho futuro, a ser realizado com a temática, desenvolvendo e atualizando os elementos e contributos já oferecidos.

9.4 – Obstáculos do trabalho

Todo trabalho de pesquisa científica possui vários obstáculos, sejam oriundos do ambiente externo ou até mesmo do próprio pesquisador. Existiram um conjunto de desafios a ultrapassar, sendo que as principais barreiras que tivemos no decorrer do percurso são:

- Encontrar artigos e textos científicos confiáveis e atualizados, já que a extração de conteúdo que envolve números precisa de ser sempre comprada e atualizada. Na área de cibersegurança, muitas das estatística e informação mais atual é reservada e implica com aspetos associados com a própria segurança e combate ao cibercrime. Tal, é normal e adequado, mas coloca alguns desafios para a obtenção de informação relevante e atual;
- Burocracia, imposto demoras e dificuldade em conseguir autorização da comissão de ética da plataforma Brasil e outros elementos, pelo que se optou por realizar os questionários apenas dirigidos aos pais e responsáveis pelos adolescentes e não aos próprios adolescentes, a quem teria de ser obtida a autorização dos próprios e dos seus responsáveis;
- Convencer os participantes a preencherem os questionários *online* ou manualmente, assegurando o respeito pelo sigilo e relevância na partilha de elementos sobre os seus descendentes ou tutelados. Em complemento, explicar que se trata de uma pesquisa e tirar as dúvidas dos participantes na hora de preenchimento do questionário;
- Eliminar questionários que foram preenchidos sem que houvesse os requisitos para participar, desde a não existência de adolescente sob responsabilidade, ao não preenchimento da totalidade das questões apresentadas, ou ainda, da suspeita de inconsistência nas respostas realizadas. Garantir a eliminação dos questionários que vinham com respostas totalmente contrárias ao que tinha sido questionado, tendo sido verificado se as informações prestadas tinham uma lógica aceitável;
- Tempo para conciliar trabalho, responsabilidade do lar e estudos, bem como, ressaltar que, durante uma fase significativa do trabalho, foi necessário lidar com os desafios adicionais colocados pelo Covid-19.

9.5 – Contributos do trabalho

A principal contribuição deste trabalho é a proposta de um modelo de prevenção de cibersegurança, a partir da criação de uma cartilha de prevenção, para que os pais, professores, responsáveis legais e quem se interessar no tema, possam ter conhecimento para prevenir e evitar que os seus adolescentes sejam vitimizados pelos cibercriminosos.

Uma vez apresentada a cartilha, podemos ir em busca de divulgar para o maior número de pessoas, incluindo a amostra desta nas escolas, fazendo com que sejam utilizadas em sala de aula também por professores, para que sejam multiplicadores de um conteúdo de potencial relevância social. Pretende-se assim, contribuir também na preparação intelectual dos adolescente, com objetivo de os conscientizar dos perigos que a rede mundial de computadores, a Internet/Web, traz e, que devem ter cuidados essenciais para que não sejam vítimas, e em último caso, se forem vítima, onde e como procurarem ajuda das autoridades competentes.

Posteriormente, podemos pensar em procurar membros do governo para que a cartilha se possa espalhar para todo o Estado do Pará, não ficando limitado somente ao município de Belém, o qual foi nossa fonte de recolha de dados. Assim, teremos a oportunidade de atingir um maior número de pessoas, já que o principal objetivo dessa longínqua pesquisa é trazer conhecimentos de cibersegurança para a população, em especial aos adolescentes, já que estes se encontram em um momento delicado de transformação da vida, e por isso são considerados mais vulneráveis à ocorrência de cibercrimes.

Importante salientar que, o preenchimento do formulário de quesitos, quando aplicado aos pais e responsáveis legais, foi bem aceite, entendido pelos participantes como uma pesquisa de alguém que se preocupa com a saúde física, e principalmente, mental dos adolescentes. Todo o processo se traduz por um retorno social bem tangível, tendo em vista que, uma vez vitimizado por um crime cibernético, tal pode trazer a um adolescente, consequências desastrosas que irão impactar por toda a sua vida.

Por último, mas não menos importante, temos que ressaltar que, foi feito um esforço significativo para recolha de dados, já que muitos participantes, ao menos tem controle ou, até mesmo, conhecimento do comportamento de seus filhos quando estão navegando na Internet. Logo, de imediato, tivemos que explicar as perguntas do questionário, começando assim já a propagar conteúdos sobre cibercrimes, fazendo com que seja "plantada uma sementinha" de conhecimento sobre o assunto. Contamos que a cartilha, uma vez produzida, seja bem aceite, já que se trata de um tema delicado e de pouco divulgação mas, de acordo com os dados recolhidos, com um potencial de ser bem recebida.

9.6 – Trabalho futuro

Acreditamos que está proposta de fazermos uma cartilha e promovermos a divulgação do tema cibersegurança para os adolescentes, pode evoluir a ponto de chegar a um manual de informação, mais completo, o qual poderá abordar de forma mais detalhada um leque alargado de informação que passará por conceitos relacionados as tecnologias de informação e comunicação, à Internet, as doenças físicas e psíquicas e demais riscos associados com o mau uso das tecnologias digitais, a aplicação penal aos delitos praticados e, finalmente, as orientações detalhadas de como agir em situação em que os adolescentes sejam vítimas de cibercriminosos.

Diante estas colocações podemos detalhar como projeto futuro os seguintes trabalhos adicionais:

- Criação de um manual mais completo de cibercrimes e cibersegurança;
- Divulgação de material em escolas pública e privadas;
- Elaboração de palestras sobre o tema;
- Incentivar o governo a produzir o manual e fornecer de forma gratuita para o maior número de pessoas possíveis;
- Utilizar as redes sociais para expandir o conteúdo para outras localidades;
- Fazer a tradução para o inglês, para que o conteúdo seja divulgado em outros países.

Lista de publicações

Em revista científica:

- Machado, T. and Gouveia, L. (2021). Covid-19 effects on cybersecurity issues. International Journal of Advanced Engineering Research and Science (IJAERS). Vol. 8, N. 8, pp 222-229, August. ISSN: 2349-6495. DOI: 10.22161/ijaers.88.27
- Machado, T. e Gouveia, L. (2021). Ameaças e vulnerabilidades associadas aos cibercrimes com crianças e adolescentes. International Journal of Advanced Engineering Research and Science (IJAERS). Vol. 8, N. 9, pp 68-77, September. ISSN: 2349-6495. DOI: 10.22161/ijaers.89.7

Em livro:

- Machado, T. Gouveia, L. (2022). A Adolescência e o Ciberespaço: comunicação de prevenções e risco de concretização de cibercrimes. Livro - EQUIDADE, CIDADANIA E EDUCAÇÃO INCLUSIVA, páginas 211-226. Editora Conhecimento. Belo Horizonte (2022).

Em relatório interno:

- Machado, T. Gouveia, L. (2021). Questionário a pais ou responsáveis sobre cibersegurança de adolescentes, na cidade de Belém do Pará no Brasil. Teste Piloto. Relatório Interno TRS 04/2021. Outubro. *TRS - Tecnologia, Redes e Sociedade. Universidade Fernando Pessoa. HANDLE: 10284/10315

Em seminário científico:

- Machado, T. e Gouveia, L. (2020). Impacto digital no crime. Seminário do Programa de Doutoramento em Ciência da Informação. Especialidade de Sistemas, Tecnologias e Gestão da Informação (SiTEGI). Universidade Fernando Pessoa. Webinar. 10 de Julho. HANDLE: 10284/8894

Referências

ABRANTES, Steven Lopes. *O m-learning no context do Ensino Superior. Uma proposta para a sua avaliação em ambientes colaborati*vos. Recuperado em 27 de janeiro, 2022, from *https://bdigital.ufp.pt/handle/10284/2242*.

ABUKARI, Arnold Mashud; BANKAS, Edem Kwedzo. *Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond*. Recuperado em 18 de julho, 2020, from *https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond*.

AHMAD, Tabrez. *Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. Recuperado em 12 de julho, 2020, from *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830.*

ALFREDO, Pereira. *O Governo Electrónico Local no Contexto de Angola: proposta de um modelo conceptual*. Recuperado em 28 de janeiro, 2022, from *https://bdigital.ufp.pt/handle/10284/4793.*

ALMEIDA, J., MENDONÇA, A., Carmo, G., Santos, K., SILVA, L. e Azevedo, R. *Crimes Cibernéticos,* Recuperado em 08 de agosto, 2018, from *https://periodicos.set.edu.br/index.php/cadernohumanas/article/view/2013*.

AMARAL, Vera Lúcia do. *A Psicologia da adolescência*. Recuperado em 15 de setembro, 2021, from *http://www.ead.uepb.edu.br/arquivos/cursos/Geografia_PAR_UAB/Fasciculos%20-%20Material/Psicologia_Educacao/Psi_Ed_A05_J_GR_20112007.pdf.*

ANTONELLI, Humberto Lidio e ALMEIDA, Emerson Gervásio de. *A Internet e o Direito: Uma abordagem sobre cibercrimes*. Recuperado em 14 de agosto, 2018, from *http://www.egov.ufsc.br/portal/sites/default/files/a_Internet_e_o_direito_uma_abordagem_sobre_cibercrimes.pdf.*

BALDISSERA, Olivia. *O QUE TODO EDUCADOR PRECISA SABER SOBRE DESENVOLVIMENTO COGNITIVO*. Recuperado em 04 de novembro, 2023, from *https://poseducacao.unisinos.br/blog/desenvolvimento-cognitivo#:~:text=O%20desenvolvimento%20cognitivo%20%C3%A9%20o,relacionados%20ao%20amadurecimento%20do%20c%C3%A9rebro*.

BARROS, Arthur de Alvarenga; CARMO, Michelle Fernanda Alves do; SILVA, Rafaela Luiza da. *A Influência das Redes Sociaise seu Papel na Sociedade*. Recuperado em 22 de novembro, 2020, from *http://www.periodicos.letras.ufmg.br/index.php/ueadsl/article/viewFile/3031/2989.*

BELCIC, Ivan. *O guia essencial sobre phishing: Como funciona e como se proteger*. Recuperado em 12 de julho, 2020, from *https://www.avast.com/pt-br/c-phishing#topic-1*.

BERGMAN, Michael K. *The Deep Web: Surfacing Hidden Value*. Recuperado em 07 de agosto, 2018, from *http://brightplanet.com/wp-content/uploads/2012/03/12550176481-deepwebwhitepaper1.pdf.*

BONAVIDES, Paulo. *Ciência Política*. 19 ed. São Paulo: Malheiros, 2012.

BORELLI, Alessandra. *Com internet, responsabilidade de escolas extrapola seus domínios*. Recuperado em 17 de novembro, 2020, from *https://www.conjur.com.br/2016-mai-16/internet-responsabilidade-escolas-extrapola-dominios*.

CAMPOS, Lorraine Vilela. *"O que são Fake News?"; Brasil Escola*. Recuperado em 10 de janeiro, 2022, from *https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm*.

CARONI, Mariana Malheiros; BASTOS, Olga Maria. *Adolescência e autonomia: conceitos, definições e desafios*. Recuperado em 16 de setembro, 2021, from *http://revistadepediatriasoperj.org.br/detalhe_artigo.asp?id=641*.

CARVALHO, Renato Gil; Novo, ROSA Ferreira. *Características da personalidade e relacionamento interpessoal na adolescência*. Recuperado em 15 de setembro, 2021, from *https://www.redalyc.org/pdf/3350/335027504005.pdf.*

CAVALCANTE, Márcio André Lopes. *Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático.* Recuperado em 16 de novembro, 2020, from *https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html*

CELLARD. A. *A análise documental*. In: J. Poupart, et al. (Orgs.). "*A pesquisa qualitativa: enfoques epistemológicos e metodológicos*." Petrópolis: Vozes, 2008.

CHAMA, Débora Corrêa. *O Comitê Gestor da Internet no Brasil: Gestão, Segurança e Comunicação*. Recuperado em 13 de agosto, 2018, from *https://repositorio.unesp.br/bitstream/handle/11449/89435/chama_dc_me_bauru.pdf?sequence=1&isAllowed=y.*

COSTA, Rogério da. *Por um novo conceito de comunidade: redes sociais, comunidades pessoais, inteligência coletiva*. Recuperado em 10 de janeiro, 2022, from *https://www.scielo.br/j/icse/a/gx3Z8FPYVqJYdN6kDZ3HyfM/?lang=pt#.*

CRAIDE, Sabrina. *Pais devem acompanhar o acesso de crianças à internet, alertam especialistas*. Recuperado em 20 de novembro, 2020, from *https://agenciabrasil.ebc.com.br/geral/noticia/2017-07/pais-devem-acompanhar-o-acesso-de-criancas-internet-alertam-especialistas.*

DESLANDES, Suely Ferreira; COUTINHO, Tiago. *O uso intensivo da Internet por crianças e adolescentes no contexto da Covid-19 e os riscos para violências autoinflingidas*. Recuperado em 17 de julho, 2020, from *https://www.scielo.br/scielo.php?pid=S1413-81232020006702479&script=sci_arttext.*

DIAS, Cristina Maria de Souza Brito; HORA, Flávia Fernanda Araújo da; AGUIAR, Ana Gabriela de Souza. *Jovens criados por avós e por um ou ambos os pais*. Recuperado em 17 de setembro, 2021, from *http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1516-36872010000200013.*

DIAS, Vanina Costa; et al. Rosa da. *Adolescentes na Rede: Riscos ou Ritos de Passagem?*. Recuperado em 15 de setembro, 2021, from *https://www.scielo.br/j/pcp/a/8W8S8XfkQWCmYNTrjCvwQkg/?lang=pt.*

DOMINGUES, Vinícius. *Em tempos de pandemia, é preciso ter muita atenção com os cibercrimes*. Recuperado em 11 de julho, 2020, from *https://www.conjur.com.br/2020-mai-13/domingues-cibercrimes-tempos-pandemia.*

DUARTE. N. *Vigotski e a pedagogia histórico-crítica: a questão do desenvolvimento psíquico*. Nuances: estudos sobre Educação, Presidente Prudente, v. 24, n. 1, p. 19-29, jan./abr. 2013.

EISENSTEIN E, Estefenon S. *Computador: ponte social ou abuso virtual?*. Adolesc Saude. 2006;3(3):57-60. Recuperado em 09 de abril, 2019, from *http://adolescenciaesaude.com/detalhe_artigo.asp?id=136.*

ELIEZER, Cristina Rezende; GARCIA, Tonyel de Pádua. *O Novo Crime de Invasão de Dispositivo Informático*. Recuperado em 16 de novembro, 2020, from *https://periodicos.uniformg.edu.br:21011/ojs/index.php/cursodireitouniformg/article/view/242*

FERNANDES, Maria Rayane de Oliveira. *A influência da mídia nos casos de grande comoção social e no processo penal*. Recuperado em 20 de novembro, 2020, from *https://jus.com.br/artigos/50786/a-influencia-da-midia-nos-casos-de-grande-comocao-social-e-no-processo-penal.*

FEUSER, Bruna Ceccone; et al.. *A Vulnersabilidade da Criança e do Adolescente nas Redes Sociais: necessária cautela para a segurança do público infanto-juvenil*. Recuperado em 01 de maio, 2020, from *http://periodicos.unibave.net/index.php/constituicaoejustica/article/view/115.*

FGV Direito Rio. *Tecnologia e Sociedade no Século XXI*. Recuperado em 10 de janeiro, 2019, from *https://plataforma9.com/publicacoes/seminario-portugal-brasil-tecnologia-e-sociedade-no-seculo-xxi.htm.*

FONSECA, Franciele Fagundes; SENA, Ramony Kris R.; SANTOS, Rocky Lane A. dos; ORLENE, Veloso Dias; COSTA, Simone de Melo. *As vulnerabilidades na infância e adolescência e as políticas públicas brasileiras de intervenção*. Recuperado em 30 de março, 2020, from *https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-05822013000200019.*

GANDRA, Alana. *Procuradora destaca importância de educação e cidadania na internet*. Recuperado em 19 de novembro, 2020, from *https://agenciabrasil.ebc.com.br/geral/noticia/2020-02/procuradora-destaca-importancia-de-educacao-e-cidadania-na-internet.*

GIBSON, Willian. *Neuromancer*. São Paulo: Aleph, 2003.

GONÇALVES, Victor Minarini. *Vitimologia: Conceituação e Aplicabilidade*. Recuperado em 17 de julho, 2020, from *https://jus.com.br/artigos/36073/vitimologia-conceituacao-e-aplicabilidade.*

GONTIJO, Cynthia Rúbia Braga et al. *Ciberespaço: que território é esse?* Recuperado em 10 de janeiro, 2022, from *http://ticsproeja.pbworks.com/f/Ciberespaco.pdf*.

GOUVEIA, Luis Borges. *Covid-19 e Desafios para a Cibersegurança num Tempo pós-Pandemia*. Recuperado em 17 de julho, 2020, from *https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20julho%202020%204%C2%AAvers%C3%A3o.pdf*

GOUVEIA, Luis Borges. *Sociedade da Informação: Notas de contribuição para uma definição operacional*. Recuperado em 07 de agosto, 2018, from *http://homepage.ufp.pt/lmbg/reserva/lbg_socinformacao04.pdf*.

INEP. *80% dos utilizadores de internet participam em redes sociais – 2019*. Recuperado em 08 de fevereiro, 2022, from *https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=354447153&DESTAQUESmodo=2*.

JESUS, Helder Fialho de. *Ciberespaço e Mundo Físico – As Duas Faces da Mesma Moeda*. Recuperado em 19 de julho, 2020, from *https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20julho%202020%204%C2%AAvers%C3%A3o.pdf*

JUNIOR, Antonio Augusto Pinto et al. *Traços de personalidade de adolescentes infratores e vitimizados por meio do Eysenck Personality Questionnaire Junior (EPQ-J*) Recuperado em 16 de setembro, 2021, from *https://www.metodista.br/revistas/revistas-metodista/index.php/MUD/article/view/9979/7118*.

JUNQUEIRA, Isabela Tavares. *Família recasada: o lugar do padrasto na perspectiva dos adolescentes*. Recuperado em 18 de setembro, 2021, from *https://www.maxwell.vrac.puc-rio.br/30396/30396.PDF*.

KASPERSKY. *O que é cibersegurança?*. Recuperado em 09 de novembro, 2020, from *https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security*.

KIEFER, Sandra. Exagero de tecnologia deixa crianças e adolescentes desconectados do mundo real. Recuperado em 04 de fevereiro, 2023, from *https://www.em.com.br/app/noticia/gerais/2014/05/25/interna_gerais,532336/exagero-de-tecnologia-deixa-criancas-e-adolescentes-desconectados-do-mundo-real.shtml*.

KLUNCK, Patrícia; AZAMBUJA, Maria Regina Fay de. *O ABANDONO DIGITAL DE CRIANÇAS E ADOLESCENTES E SUAS IMPLICAÇÕES JURÍDICAS*. Recuperado em 05 de dezembro, 2020, from *https://www.pucrs.br/direito/wp-content/uploads/sites/11/2020/04/patricia_klunck.pdf*.

KOHN, Karen; MORAES, Cláudia Herte de. *O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital*. Recuperado em 07 de agosto, 2018, from *http://www.egov.ufsc.br/portal/sites/default/files/o_impacto_das_novas_tecnologias_na_sociedade.pdf*.

KRIPKA, Rosana Maria Luvezut; SCHELLER, Morgana; BONOTTO, Danusa de Lara. *Pesquisa Documental: considerações sobre conceitos e características na Pesquisa*

Qualitativa. Recuperado em 26 de setembro, 2021, from *https://proceedings.ciaiq.org/index.php/ciaiq2015/article/view/252/248.*

LANCASTER, F. W. *O currículo da Ciência da Informação*. Revista de Biblioteconomia de Brasília, Brasília, v. 17, n.1, p. 01-05, jan./jun. 1989.

MACEDO, Fernanda Beatriz Ferreira de. *Falando a Gente Encontra a Solução: Estudo de Caso Sobre a Percepção dos Alunos e Alunas Participantes do Projeto Crimes Virtuais*. Recuperado em 17 de novembro, 2020, from *https://www.udesc.br/arquivos /faed/id_cpmenu/251/fernanda_beatriz_ferreira_de_macedo_15688165832336_251.pdf.*

MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático: A especial vulnerabilidade das crianças e dos adolescentes*. Recuperado em 07 de agosto, 2018, from *https://bdigital.ufp.pt/handle/10284/6089.*

MALAVÉ, Mayra Malavé. *O papel das redes sociais durante a pandemia*. Recuperado em 11 de julho, 2020, from *http://www.iff.fiocruz.br/index.php/8-noticias/675-papel-redes-sociais*.

MANCILLA, Omar Reyes. *A Importância da Internet para o Desenvolvimento das Vendas no Brasil*. Recuperado em 10 de janeiro, 2022, from *https://cepein.femanet.com.br/BDigital/arqTccs/1111390013.pdf.*

MARTINS, Heloisa Helena T. de Souza. Martins. *Metodologia qualitativa de pesquisa*. Recuperado em 26 de setembro, 2021, from *https://www.scielo.br/j/ep/a/4jbGxKMDjKq79VqwQ6t6Ppp/?format=pdf&lang=pt*.

MARTINS, Marina; CARVALHO, Carolina. *A MENTIRA NA ADOLESCÊNCIA: UMA ANÁLISE BASEADA NO CONTEXTO SOCIAL*. Recuperado em 16 de setembro, 2021, from *https://www.researchgate.net/publication/268223464_A_MENTIRA_NA_ADOLESCENCIA_ UMA_ANALISE_BASEADA_NO_CONTEXTO_SOCIAL/link/546643d50cf25b85d17f5e71/do wnload*.

MATOS, Margarida Gaspar de; et al. *Os Adolescentes Portugueses, A Internet e as Dependências Tecnológicas*. Recuperado em 10 de janeiro, 2022, from *https://repositorio.ul.pt/handle/10451/38156.*

MEDEIROS, Marcos Fernando M., NETO, Manoel Veras de Sousa. *Computação em nuvem e governança da Internet no governo brasileiro: um estudo de caso com gestores de TI*. Recuperado em 09 de novembro, 2020, from *https://core.ac.uk/download/pdf/230223204.pdf*.

MENDOZA, Miguel Ángel. *Os 10 principais riscos na Internet para crianças e adolescentes*. Recuperado em 03 de maio, 2020, from *https://www.welivesecurity.com/br/2018/ 05/21/principais-riscos-na-Internet-para-criancas-e-adolescentes/.*

MEDICINA NET. Conceito extraído da Classificação Internacional de Doenças (CID) da Organização Mundial de Saúde (OMS). Recuperado em 25 de abril, 2019, from *https://www.medicinanet.com.br/cid10/5473/f654_pedofilia.htm*

MILITÃO, Octávio Pimenta. *Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional*. Recuperado em 09 de novembro, 2020, from *https://run.unl.pt/bitstream/10362/14300/1/Dissertacao_OMilitao_35664.pdf.*

MICROSOFT. *Microsoft Defender Antivírus no Windows*. Recuperado em 10 de janeiro, 2022, from *https://docs.microsoft.com/pt-br/microsoft-365/security/defender-endpoint/micro soft-defender-antivirus-windows?view=o365-worldwide*.

MINHAVIDA. *Saúde de A a Z.* Recuperado em 10 de janeiro, 2022, from *https://www.minhavida.com.br/saude/temas/a-z/d.*

MISKOLCI, Richard. *Sociologia Digital: notas sobre pesquisa na era da conectividade*. Contemporânea – Revista de Sociologia da UFSCar. Recuperado em 09 de agosto, 2018, from *https://www.contemporanea.ufscar.br/index.php/contemporanea/article/view/525*.

MONTEIRO, Ana Francisca Cunha. *A Internet na Vida das Crianças: como lidar com perigos e oportunidades*. Recuperado em 25 de junho, 2019, from *encurtador.com.br/abqKT.*

MOREIRA, Jacqueline de Oliveira. *Mídia e Psicologia: considerações sobre a influência da internet na subjetividade*. Recuperado em 20 de novembro, 2020, from *http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1870-350X2010000200009.*

MORGADO, Alice Murteira; DIAS, Maria da Luz Vale. *Comportamento Antissocial na Adolescência: o papel de características individuais num fenómeno social*. Recuperado em 14 de setembro, 2021, from *https://www.researchgate.net/publication/301220767_ Comportamento_antissocial_na_adolescencia_O_papel_de_caracteristicas_individuais_num _fenomeno_social_Antisocial_behaviour_in_adolescence_The_role_of_individual_characteri stics_on_a_social_phenomenon.*

MOTA, Catarina Pinheiro; FERREIRA, Sara Duarte. *Estilos parentais, competências sociais e o papel mediador da personalidade em adolescentes e jovens adultos*. Recuperado em 17 de setembro, 2021, from *https://repositorio-aberto.up.pt/bitstream/10216/124368/2/368108.pdf.*

NAIDOO, Rennie. *A multi-level influence model of COVID-19 themed cybercrime*. Recuperado em 09 de julho, 2020, from *https://orsociety.tandfonline.com/doi/full/10.1080/0960085X.2020.1771222.*

NATIONAL INSTITUTE OF STANDARDS AND TECNOLOGY. *Computação em Nuvem*. Recuperado em 09 de novembro, 2020, from *https://csrc.nist.gov/Projects/Cloud-Computing*.

NIPPES, Gabriel; GUIDOLINI, Paulo Octavio. O dilema do capitalismo de vigilância. Recuperado em 10 de janeiro, 2022, from *https://periodicos.ufes.br /peteconomia/article/view/33792.*

OLIVEIRA, Eloiza Silva Gomes. *Adolescência, Internet e tempo: desafios para a Educação*. Recuperado em 10 de novembro, 2020, from *https://www.scielo.br/pdf/er/n64/0104-4060-er-64-00283.pdf.*

OLIVEIRA, Maria Marly de. *Como Fazer Pesquisa Qualitativa*. 7. Ed. Petrópolis, RJ: Vozes, 2018.

PELARIGO, João Ferreira. *Os dez (10) desafios mais perigosos da internet*. Recuperado em 10 de janeiro, 2022, from *https://cipave.rs.gov.br/os-dez-10-desafios-mais-perigosos-da-internet.*

PEREIRA, Marília do Nascimento. *A Superexposição de crianças e adolescentes nas redes sociais: necessária cautela no uso das novas tecnologias para a formação de identidade*. Recuperado em 10 de maio, 2020, from *http://coral.ufsm.br/congressodireito/anais/2015/6-14.pdf.*

PINHEIRO, Patricia Peck. 2013. *Direito Digital*, 5ª ed. São Paulo. Saraiva.

POMPÉO, Wagner Augusto Hundertmarck; SEEFELDT, João Pedro. *Nem tudo está no Google: deep Web e o perigo da invisibilidade*. Recuperado em 10 de janeiro, 2022, from *http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf.*

PONTES, Cristina; BATISTA, Susana. BAPTISTA, Rita. Portugal 1ª ronda questionário – 2021. Recuperado em 10 de março, 2022, from *https://zenodo.org/record /6010478#.YgU8vd_MJPY.*

PRATTA, Elisângela Maria Machado; SANTOS, Manoel Antônio dos. *Família e adolescência: a influência do contexto familiar no desenvolvimento psicológico de seus membros*. Recuperado em 17 de setembro, 2021, from *https://www.scielo.br/j/pe/a/3sGdvzqtVmGB3nMgCQDVBgL/?lang=pt.*

RAHAL, Carla; TURRINI, Janaína; FIORESE, Urbano; FURTADO, Felipe. *Crimes digitais e prevenção em época de pandemia*. Recuperado em 12 de julho, 2020, from *https://cryptoid.com.br/banco-de-noticias/crimes-digitais-e-prevencao-em-epoca-de-pandemia/.*

RIBEIRO, Gustavo Lins. *Medo Global. Boletim n. 5. Cientistas sociais e o coronavírus*. Anpocs. Recuperado em 14 de julho, 2020, from *http://www.anpocs.com/index.php/ciencias-sociais/destaques/2311-boletim-n-3.*

RODRIGUES, Renato. *Brasil é líder em empresas atacadas por ransomware na epidemia*. Recuperado em 11 de julho, 2020, from *https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/.*

SAFERNET. *O que é sextorsão?*. Recuperado em 10 de janeiro, 2022, from *https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o#mobile*.

SALLES, Leila Maria Ferreira. *Infância e adolescência na sociedade contemporânea: alguns apontamentos*. Recuperado em 17 de setembro, 2021, from *https://www.researchgate.net/publication/237972961_Infancia_e_adolescencia_na_sociedade_contemporanea_alguns_apontamentos*.

SANCHES, Ademir Gasques; ANGELO, Ana Elisa de. *Insuficiência das leis em relação aos crimes cibernéticos no Brasil*. Recuperado em 22 de novembro, 2020, from *https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil*.

SANTOS, Edméa O. *EAD, palavra proibida. Educação online, pouca gente sabe o que é. Ensino remoto, o que temos para hoje. Mas qual é mesmo a diferença?*. Revista Docência e Cibercultura. 2020.
SANTOS, Letícia Dutra de Oliveira. *POLÍTICAS PÚBLICAS DE EDUCAÇÃO DIGITAL: Prevenção e Combate aos Crimes Cibernéticos*. Recuperado em 03 de fevereiro, 2023, from *http://45.4.96.19/bitstream/aee/10044/1/LET%c3%8dCIA%20DUTRA%20DE%20OLIVEIRA%20SANTOS.pdf.*

SANTOS, Luiz Carlos dos. *Pesquisa Científica: universo/população, amostra e critério amostral*. Recuperado em 07 de outubro, 2021, from *http://www.lcsantos.pro.br/wp-content/uploads/2021/03/195_PESQUISA_CIENTIFICA.pdf*.

SERAFINI, Adriana Jung. *Satisfação de Vida, Rede de Relações, Coping e Neuroticismo em Adolescentes Portadores e não Portadores do Vírus de Imunodeficiência Humana – HIV*. Recuperado em 15 de setembro, 2021, from *https://www.lume.ufrgs.br/handle/10183/15390*.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallas Tomaz. *Relações Jurídicas Virtuais: Análise de Crimes cometidos por meio do uso do da Internet*. Recuperado em 25 de abril, 2019, from *http://egov.ufsc.br/portal/sites/default/files/3952-21333-1-pb.pdf*.

SILVA, Eugénio Alves. *Educação, Gestão Escolar e Projecto Educativo*. Educação e Desenvolvimento Local. 1º Fórum Provincial da Educação da Huila. ECO7 Investimentos, Lda. Luanda, 2017.

SILVA, Rosane Leal da; Veronese, Josiane Rose Petry. *Os crimes sexuais contra criança e adolescente no ambiente virtual*. Recuperado em 19 de abril, 2019, from *https://ambitojuridico.com.br/edicoes/revista-69/os-crimes-sexuais-contra-criancas-e-adolescentes-no-ambiente-virtual/*

SILVA, Thayse de Oliveria e SILVA, lebian Tamar Gomes. *Os impactos sociais, cognitivos e afetivos sobre a geração de adolescentes conectados às tecnologias digitais*. Recuperado em 09 de agosto, 2018, from *http://pepsic.bvsalud.org/pdf/psicoped/v34n103/09.pdf*.

SILVA, Vanessa Toste Soares da. *Sociedade Digital - O Poder da Multidão Participativa*. Recuperado em 11 de janeiro, 2019, from *https://ubibliorum.ubi.pt/bitstream/10400.6/1584/1/Tese_Mestrado_Vanessa_Silva.pdf.*

SOUSA, Daniela Heitzmann Amaral Valentim de; DIAS, Cristina Maria de Souza Brito. *Recasamento: percepções e vivências dos filhos do primeiro casamento*. Recuperado em 17 de setembro, 2021, from *https://www.scielo.br/j/estpsi/a/phvVZrg9QrCTG5k9yKS9HJD/?lang=pt.*

SOUZA, Dercia Antunes de; OLIVEIRA, Joyce Alessandra de Moraes. *Uso de Tecnologias Digitais por Crianças e Adolescentes: potenciais ameaças em seus inter -relacionamentos*. Recuperado em 01 de maio, 2020, from *https://www.aedb.br/seget/arquivos/artigos16/952473.pdf*

TIBÚRCIO, Lara Pinto. *Novos Desafios Frente a Legislação Civil: o impacto do meio digital no dever de vigilância parental*. Recuperado em 22 de novembro, 2020, from *https://periodicos.uni7.edu.br/index.php/iniciacao-cientifica/article/view/750.*

TRIPP, David. *Pesquisa-ação: uma introdução metodológica*. Recuperado em 28 de janeiro, 2022, from *https://www.scielo.br/j/ep/a/3DkbXnqBQqyq5bV4TCL9NSH/?format=pdf&lang=pt.*

TRUZZI, Gisele. Cyberbullying, Cyberstalking e Redes Sociais. Recuperado em 10 de janeiro, 2022, from *https://fernandafav.jusbrasil.com.br/noticias/140330213/cyberbullying-cyberstalking-e-redes-sociais-os-reflexos-da-perseguicao-digital.*

ULLOA, Estefany Lizet León. *Neuroticismo como factor asociado a la adicción al Internet en Adolescentes de colegios públicos de Trujillo*. Recuperado em 15 de setembro, 2021, from *http://repositorio.upao.edu.pe/handle/20.500.12759/5973.*

UNIC Rio de Janeiro. *'Internet das coisas' pode levar países emergentes a superar desafios de desenvolvimento, aponta ONU*. Recuperado em 05 de fevereiro, 2021, from *https://unicrio.org.br/internet-das-coisas-pode-levar-paises-emergentes-a-superar-desafios-de-desenvolvimento-aponta-onu/.*

UNICEF, Fundo das Nações Unidas para a Infância. *O Uso da Internet por Adolescentes*. Recuperado em 11 de novembro, 2020, from *https://crianca.mppr.mp.br/arquivos/File/publi/unicef/br_uso_Internet_adolescentes.pdf.*

VIANNA, Túlio Lima. *Dos crimes pela Internet*. Recuperado em 09 de agosto, 2018, from *http://www.alfa-redi.org/sites/default/files/articles/files/vianna.pdf.*

YOBA, Carlos Pedro Cláver. *Participação da família e da escola na educação dos jovens*. Recuperado em 04 de fevereiro, 2023, from *http://pepsic.bvsalud.org/pdf/cp/v26n27/03.pdf*.

Legislação consultada

BRASIL. Lei 2.848, de 7 de dezembro de 1940. Recuperado em 10 de janeiro, 2022, from *http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm*.

BRASIL. *Constituição da República Federativa do Brasil De 1988*. Recuperado em 22 de novembro, 2020, from *http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm*.

BRASIL. Lei nº 8.609, de 13 de julho de 1990. Recuperado em 25 de abril de 2018, from *http://www.planalto.gov.br/ccivil_03/leis/L8069.htm.*

BRASIL. Lei 9.394, de 20 de dezembro de 1996. Recuperado em 17 de novembro, 2020, from *http://www.planalto.gov.br/ccivil_03/leis/l9394.htm.*

BRASIL. Lei 13.185, de 6 de novembro de 2015. Recuperado em 17 de novembro, 2020, from *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm*.

BRASIL. Decreto lei nº 9.637, de 26 de dezembro de 2018. Recuperado em 10 de março, 2022, from *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm*.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Recuperado em 11 de julho, 2020, from *http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.*

BRASIL. Decreto lei nº 10.748, de 16 de julho de 2021. Recuperado em 10 de março, 2022, from *http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm*.

No contexto do trabalho realizado, foram publicados os seguintes trabalhos:

International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-8, Issue-8; Aug, 2021
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.88.27

Covid-19 effects on cybersecurity issues

Thiago José Ximenes Machado[1], Luís Borges Gouveia[2]

[1]Technologist in Data Processing; Bachelor in Law; Post-Graduated in: Computer Networking; Digital Forensics and Computer Forensics (in progress); Criminal Law and Criminal Procedural Law; Criminology; Criminal Sciences; Public Safety Policy and Management; Electronic Law; Constitutional Law (in progress) Master in Criminology and PhD in Information Science (in progress) - Fernando Pessoa University - Porto City (Portugal).
[2]Luis Borges Gouveia. Completed the Academic Title of Aggragate in 2010 by the Universidade de Aveiro and the Doctorate in Computer Sciences in 2002 by the Lancaster University (United Kingdom) and the Masters in Electrotechnical and Computers Engineering in 1995 by the Universidade do Porto. Full Professor at the Universidade Fernando Pessoa.

Received: 02 Jul 2021,
Received in revised form: 08 Aug 2021,
Accepted: 15 Aug 2021,
Available online: 21 Aug 2021

Keywords— ***Pandemic, Cybercrimes, Vulnerable, Cybercrimes, Technology, Internet, Cyberspace.***

Abstract— *This scientific initiation article will bring up current and very relevant questions about the effects suffered in the virtual world after the announcement of a pandemic, with regard to the growing number of crimes committed by virtual means, considering that the use of the internet for practically any and all daily activities became mandatory. We will show the activities that needed to adapt to the new reality, as well as the increase in cybercrime that came to affect, in particular, those whose expertise and technological knowledge do not match reality. We will also talk about the victims of these crimes and conclude with a cybersecurity protocol which can be applied to minimize risks and hinder the actions of opportunistic offenders.*

I. INTRODUCTION

In the 21st century, the world began to live with a somewhat limited and dark reality, making people, even those with no affinity for technology, feel the need to use digital equipment, especially those connected to the Internet. Such resources minimize idleness, facilitating the maintenance of work, educational, and other activities.

We will show the methodology that was used to develop the research for this paper and why we decided this was the best method.

First of all, we will discuss the use of technologies associated with the Internet in times of pandemics, where the potentialization of online services and the increase in the number of hours of access to the world wide web have awakened in cybercriminals an unparalleled opportunity to practice their crimes, often taking advantage of the vulnerability and lack of knowledge of Internet users.

Next, we will address the issue of criminal opportunity in the face of the new global scenario scenario, namely, the officialization of a pandemic. In this aspect, we will make a brief analysis of how cybercriminals have taken advantage of the virtual services that have become part of people's daily lives, in order to put into practice their cyberattacks and obtain illicit profits.

In the third part we will expose the criminal opportunity in the face of the new global scenario, since people, due to social isolation because of the pandemic, had the need to resort to technological resources connected to the Internet to perform their daily and work activities, becoming more vulnerable to cybercriminals who took advantage of the moment to practice cybercrime.

Continuing the subject, the fourth part brings a specific explanation about a work model called home office, which consists of obeying social isolation, making company employees work remotely from their own homes. However, we will show that due to the habit of not practicing cybersecurity protocols, they ended up being targets for cybercrimes, which brought irreparable damage to companies and organizations.

The fifth part of the article will bring to the reader a reflection on the greater vulnerability of children and adolescents in face of the greater time spent accessing the Internet in times of pandemics, since this excess, considered as something normal by the vulnerable, can bring about a digital addiction and thus lead to a series of problems, both in terms of mental health and physical integrity.

In the penultimate part, we will address a very relevant point that sometimes gets forgotten, that is, the victim being considered guilty for the cybercrimes he/she suffers. We will show that most victims of cybercrime do participate, but we cannot blame them for not having the expertise to enter the virtual world.

The last one will bring the reader two tables of protocols that can be used, both in the enterprise and in the home, to minimize the chances of being being targeted by cybercriminals.

We will end with a reflection on the consequences brought about by the worldwide spread of a deadly virus called Sars-cov-2, or simply COVID-19 or Coronavirus, which besides causing changes in real life, has brought about major changes in the activities developed in the virtual environment, that is, in cyberspace.

II. METHOD

The methodology applied was qualitative, characterized by the analysis of other articles and official documents that bring information related to the theme addressed.

From this content, extremely current, we can describe the modification which begins with the user's behavior, as well as the delinquents who, taking advantage of this pandemic moment and of people's great vulnerability, have invested in the practice of cybercrime.

The study relied on a considerable volume of scientific articles, so that the necessary knowledge was extracted from each one to develop relevant information to compose our scientific research.

Based on the explored content, we extracted several information ranging from the association of Internet use in times of pandemic to the main resources to minimize cyberattacks.

Finally, we show the conclusion that was drawn after the study and that will certainly contribute to society in general, since the connectivity, nowadays, reaches a large part of the world's population, regardless of social class.

III. RESULTS AND DISCUSSION

USE OF INTERNET-ASSOCIATED TECHNOLOGIES IN TIMES OF PANDEMIC

In face of the new scenario in which the world found itself, that is, the announcement of the spread of a virus called COVID-19, or popularly called the new CoronaVirus (Sars-cov-2), people had the need to adapt to changes in their lives, whether at home, in education, in the family, or at work.

The use of the Internet has become a more than essential tool, due to the prohibition of physical contact between people. Virtual communication has gained strength, so much so that all areas in which our lives are involved have needed to adapt, in order to reduce the damage caused by this dangerous and deadly virus.

The potential of the internet, especially social networks, has brought a series of benefits for people, as they feel the need to keep in touch with each other. Several activities have gained prominence in this current moment, lives have become a word of everyday life, where artists have found space to perform their shows, politicians run electoral campaigns, physical educators promote activities that can be performed at home, many run solidarity campaigns, and a series of entertainments that help to improve the psychological and physiological factor of those isolated by quarantine.

On the other hand, the media started to spread news of chaos and despair all over the world, and every day the news, whether on television or social networks, showed death and more deaths caused by COVID-19. And due to this excess of information, many have acquired anxiety and other psychological disorders. We can still highlight the misinformation, which leads to disbelief in science, with respect to epidemiological knowledge, as well as health guidelines, bringing more risks to the population.

Taking advantage of the intense flow that the World Wide Web is producing thanks to this new context experienced in pandemic times, the cybercriminals' attentions have turned to committing crimes practiced with the help of technological resources and equipment, making, in this moment of crisis, victims all over the world.

Due to people's desperation, and the anxiety to know how the pandemic scenario is, both globally and regionally, the evildoers began to create sites containing fake news and make available applications that had the purpose of showing viral maps, but behind these small programs, available for download, there was malware, responsible for the capture of various types of personal data.

Conferences through videos started to be used to shorten the distance between people, and for this reason the use of platforms such as Zoom increased, which fell victim to cybercriminals who discovered flaws and had access to the data of millions of users.

In Brazil we have the law 13.709/18 (General Law of Data Protection) that had its wording changed in August 2019. This, addresses the topic and provides administrative punishments to companies that do not take the necessary care to protect their users' data. Such objective is brought in the first article of this law, providing

This law provides for the processing of personal data, including in digital media, by natural persons or legal entities of public or private law, in order to protect the fundamental rights of freedom and privacy and the free development of the personality of the natural person.

We infer that technology was and is a fundamental ally for the continuity of daily activities, however, people need to be aware that the misuse of these tools can bring irreparable damage, be it to property or even psychological.

CRIMINAL OPPORTUNITY IN THE NEW WORLD SCENARIO

Even before it became a pandemic, the world learned that a deadly virus had started in China, and soon Internet users began to search for information on the subject on search engines. Thus, cybercriminals have already started to prepare for their attacks, based on the interests shown by the population in their searches.

It is important to highlight that with the family confinement that had been interrupted, the number of crimes against property and even the illicit drug trade had a considerable decrease. However, this new model of life has created a virtual refuge, that is, the cyber environment, which has its virtues and its dark side.

According to IBGE (Brazilian Institute of Geography and Statistics), there are currently approximately 220 million active smartphones in Brazil, considering that our population is around 211 million inhabitants. And using these, some services began to be operated in a more common way, such as delivery applications.

These applications have awakened criminals to lure their victims into giving them their credit card data and passwords, using a technique called phishing. This type of fraud is also used to issue fake bank slips, making users believe that they are really paying for a certain product or service, but that the amount is sent to an unknown account.

The Phishing technique has the help of another technique called Pharming, which is to direct the user to a fake site, but showing itself as a reliable copy of the original site. Thinking that he is accessing the real site, the user enters personal data related to his account, and has these stolen.

Still in this vein, a very relevant factor has been the high number of companies going bankrupt and others drastically reducing their staff. Thus, the number of unemployed people has grown, and the evildoers have taken advantage of this to lure and steal data from these people, by means of links leading to sites with false job offers, making them fill out forms with personal data, which would be stolen.

Google's official blog reported that more than 240 million spam messages were sent daily, containing the word COVID in their text, and these often directed users to the 42,000 web sites created from the beginning to the end of March (chart below), which use the same technique mentioned above to illegally capture data.

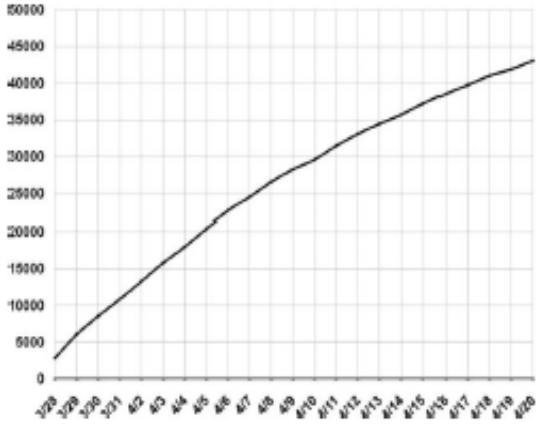


Fig.1: Cumulative number of COVID-related domains that have been registered.

Many were the fraud schemes employed by cybercriminals, characterized by the moment of desperation experienced by the world in a frantic search for the vaccine. Thus, the criminals requested contributions from Internet users so that it would be possible to create the vaccine against COVID-19, which in fact were nothing more than fraudulent gimmicks.

Another resource that has been used to negotiate products is the so-called e-commerce, where people advertise sales of the most varied things. Taking advantage of the data entered on these sites, the criminals manage, through social engineering, to trick the victims into providing codes that are sent to their cell phones, thus causing their WhatsApp application to be cloned, starting the crime of fraud, since they start asking the contacts for money, misleading the victim, because they pretend to be the owner of that account.

Due to the lack of expertise of Internet users, the social engineering technique succeeds in 80% of the scams that are applied. And the pandemic, without a doubt, has provided the ideal opportunity for cybercriminals to act, leading to a significant growth in cybercrime.

We deduce that after the WHO (World Health Organization) declared the pandemic, people started to use technologies more frequently and even unbridled, especially those connected to the Internet, since communication and physical contact became dangerous and even deadly. Thus, the barriers of distance and social isolation were minimized by virtual communications. However, along with this resource, came the problems, especially the increase in cybercrime.

THE RISKS OF HOME OFFICE FOR USERS WITH NO TECHNOLOGICAL EXPERTISE

Small and medium-sized companies were the ones that suffered most from the pandemic announcement, because, to avoid contamination among their employees, they had to take urgent measures, and, one of them was to adopt the work system called home office, which in its literal translation would be work at home.

According to the company Kaspersky, through its senior manager of social media Kaspersky - Brazil, says that "The bad news is that every time something big happens, cybercriminals take advantage of the opportunity", since employees were transferred from companies or offices to their homes without adequate protection for performing tasks over the Internet, making them easy targets to be affected by ransomware.

In an analysis, the director of Kaspersky's global research and analysis team in Latin America states that

> What cybercriminals do is attack a hospital or any other entity to steal information. Later, they encrypt it and threaten to make the stolen data stolen data public. Ashamed and afraid of the distrust and fines generated security incident like this, most organizations give in to blackmail.

He further adds "These groups are responsible for attacks on hospitals and healthcare organizations, critical services during this pandemic, but they also target banks, insurance companies, law firms, accounting firms among others and are here to stay."

For experts, these attacks have occurred with great frequency in Latin American countries, especially in Brazil, which had an increase around 350% in the first quarter of 2020, and this is due to the factor of bad corporate online access habits, of which, three stand out: use of weak passwords, use of pirated programs and lack of application of software patches.

Besides ransomware and phishing attacks, there are many other types of cybercrime that can be committed, such as data destruction, fraud, and system downtime, among others. According to specialized reports, these will cost the world $6 trillion by 2021.

Another malware widely used is the keylogger, which after being installed on the victim's computer, captures the information typed and sends it to the criminal's e-mail, as a recent example of this type of file infected with such a malicious program, we have the Eeskiri-COVID-19.chm (Estonian Rules), which apparently would show sites that help combat COVID-19.

We find that cybercriminals' expertise and opportunism are always on alert. Just as companies have visualized a way to keep their services running in the period of social isolation caused by the pandemic, so too have the criminals perfected their malicious techniques. Therefore, we must emphasize that cybersecurity protocols must always be prioritized before implementing any and all activities that involve technological resources, especially those that are directly connected to the World Wide Web.5.

THE INCREASED VULNERABILITY OF CHILDREN AND ADOLESCENTS TO LONGER INTERNET ACCESS DURING PANDEMIC TIMES

As everything had to reinvent itself in times of pandemic, education could be no different. Teachers have

been forced to use new teaching methods, even though many have never had contact with online classes. On the other hand, students had to adapt to a new classroom model, that is, distance learning, which for many is very difficult to learn this way.

Besides classes, children and teenagers have an excessive amount of time using Internet-connected technologies, and due to the large amount of information about the deadly virus, these vulnerable people can acquire a high level of stress and anxiety, since many are the conflicts that can torment their minds, which can lead to depression.

For the professor and researcher Gustavo Lins Ribeiro, the Internet with its multiple activities can provide a good or bad experience, bringing the following conclusion,

> The coronavirus pandemic is the first to be experienced in online time. The Internet, with its multiplication of the capacity of capillary communication, at the same time that it provides a global awareness, creates an expectation and paranoia in the expectation that the large numbers of sick and dead, supposedly defined in a millimeter daily, do not reach with the same intensity the places where we live.

The problem is even worse when these vulnerable people already have compromised mental health, because then the probability of idealization and suicide attempts increases. It is worth pointing out that excessive use can lead to some addictive disorders, such as cyber sex, net gaming, social networks, and others.

Another very imminent risk is that of being a victim of cyberbullying, as a result, especially for teenagers, of exposing their images with the objective of reaffirming an expectation of recognition before other internauts, and who knows, maybe even become famous as a digital influencer. However, constant criticism and insults can cause psychological damage and, not to mention, the configuration of crimes against honor.

Adolescence is a time of many discoveries, which may be accompanied by some psychological disorders, which can generate the desire for self-mutilation and even suicide, and the Internet, at this time, becomes a fertile ground for this idealization. A classic example is the challenge that became known as Blue Whale, where participants had to perform a series of tasks (challenges) and the last one was suicide.

In this same context of online challenges, in the current situation of the pandemic, where the product alcohol gel became known for being a way to eliminate the virus, they took advantage of the situation and created the "Alcohol Gel Challenge", where participants made videos inhaling, drinking, spitting the product into flames and even setting fire to their own bodies, i.e., extremely dangerous practices for health and physical integrity.

On the other hand, the criminals, using the innocence of children, began to create videos with children's cartoon characters, who communicated in a dissimulated and persuasive manner so that these vulnerable people would provide the credit card data of their parents.

We deduce that children and adolescents can become dependent on the use of technologies, especially those connected to the Internet, and that due to the scenario in which we are directly involved, social isolation associated with cybercriminals' traps can bring harm to both the vulnerable and their parents.

THE VICTIM BEING CONSIDERED GUILTY FOR CYBERCRIMES

In the criminal scenario, the victim plays an important role and should be the target of study, that is why we have victimology, which is a science that will study the role of the victim in crime. In the context of cybercrimes it is fundamental to analyze the behavior of those who have been targeted by cybercriminals.

Within the classification of victims we have: Completely innocent victim or ideal victim is the one who had no participation in the criminal action; Victim by ignorance or victim less guilty than the delinquent is the one who contributes in some way to the occurrence of the offense; Victim as guilty as the delinquent is the one whose participation in the crime is fundamental, i.e., he becomes a victim due to ambition, as much as that of the criminal; and Victim more guilty than the delinquent or provoking victim is the one who brings the blame to himself, i.e., he became a victim due almost exclusively to his own fault .

In Brazilian criminal law, the victim's behavior is taken into consideration when determining the penalty that will be attributed to the offender. However, if the victim is exclusively to blame, no penalty is applied, and the perpetrator is exempted.

As we have already studied, Internet users, especially teenagers, tend to behave inappropriately with regard to some conducts, making them partly to blame for

some of the crimes they have committed. However, we cannot blame the victim exclusively, since the criminal is someone else, and the crime cannot be justified by a possible "mistake" of the inexperienced, careless or uninformed internet user.

In many types of cybercrime, however, there is no participation of the victim, since his actions on the Internet are commonplace, and one fine day, what looked like a file sent by your bank, may be malware that will be installed on your electronic device, making you become a new victim of cybercriminals.

With the pandemic, digital communication networks have had to open up to accommodate a greater number of users, i.e. companies have had to provide access through remote tools, which are connected to the Internet. Thus, the vulnerability and amplification of risks inherent to cybercrime have increased considerably, and because of this digital acceleration in times of COVID-19 propagation, that the challenges related to cybersecurity techniques have multiplied.

With such network openings, the victims have also become more vulnerable, since, due to their lack of preparation for this new model of "virtual life", they are not very concerned about digital security issues or often rely on the structure offered by the companies where they perform their work activities.

We realize, then, that in most cases of cybercrime, the victim has a certain share of guilt, because his or her careless behavior when accessing the Internet comes as a real gift to cybercriminals, who are always on the prowl, waiting for the unwary and careless Internet users. On the other hand, we have the victims who do not contribute to the criminal action, having in their cases security flaws in the systems used.

CYBERSECURITY PROTOCOL

The use of any and all technology, especially those connected to the internet, want essential care so that this useful and practical tool does not become a hidden villain in a criminal scenario.

Cybersecurity, especially for ordinary internet users, never seemed so important, until they fell victim to the cybercriminals. And when it comes to organizations, whether public or private, this security that used to be important, is now extremely important and essential for the full functioning of their activities.

Let's start with the protection of personal computers that are used to surf the Internet and carry out everyday activities (bill payments, research, online classes, and others). In the following table we will show the main rules of digital security.

Protection Sofware	Antivirus and anti-malware programs must always be up to date and ready to detect threats.
Social Engineering	Guidance is the best weapon against this kind of attack. So it should be taught that passwords and other personal data should not be passed on to anyone via the Internet.
Education Protocol	It shows users at least the main types and techniques of attacks used by cybercriminals. These range from care when clicking on unknown links to the expertise in identifying the social engineering technique.
Security Policies	It consists of creating documents that address the policies to be followed to maintain better security. These range from monitoring to audits that will be performed on the organization's computers.
Password Manager	It is very important that users have distinct passwords for each system accessed, and that these passwords are strong, i.e. long and with several types of characters. And in order not to forget them they can use password manager programs.

As seen, it is of great importance that people, before entering the world of technologies connected to the World Wide Web, know the main concepts of security, because the terrain is very fertile for cybercriminals who take advantage exactly of this lack of knowledge to then reach their victims.

With regard to cybersecurity protocols that can be used by companies in this current scenario that makes the home office service available to their employees, we have a short list shown in the following table[1].

VPN (Virtual Private Network)	The VPN will create a tunnel, where data is encrypted, thus making it harder for intruders to decipher.
Authentication	It is important that all systems are

[1] ABUKARI, Arnold Mashud; BANKAS, Edem Kwedzo. *Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond*. Recovered in 18 de july, 2020, from https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond.

	accessed through authentication, requiring strong passwords from the user.
Protection Software	Antivirus and anti-malware programs must always be up to date and ready to detect threats.
Social Engineering	Users should be advised not to give out passwords or any data without being sure that they are talking to the real technical support.
Password Manager	It is important that companies guide their employees to use strong and different passwords for each system accessed, thus making it more difficult for cybercriminals. Password management software can be used as a resource.
Firewall	The importance of using firewall systems, as a way to prevent the invasion of computers, closing the main communication ports used by the systems.

In analysis, we can infer that we all got to know a new world scenario that was changed after the pandemic was announced, thus, both people and organizations, public or private, had to reinvent themselves in order not to enter into an economic crisis and even the decree of bankruptcy. However, due to the short period of time that everything had occurred, there was not enough time to prepare the staff to deal with the new work method, which is the resources connected to the Internet.

IV. CONCLUSION

The pandemic scenario brought to the whole world a new vision of life, changing people's behavior in their daily lives, however, the purpose of this article was to show the influences and changes brought to cyberspace, that is, the impact caused in issues related to cybersecurity, considering that the time of access to the World Wide Web has grown in an exorbitant way.

Technologies, especially those connected to the Internet, are increasingly entering our lives, whether to facilitate daily tasks, for school learning, to automate work activities, for socialization and communication between people and peoples, or even for entertainment. However, of one thing we are sure, many can no longer live without these technological resources.

With the tragic announcement of the spread of the Sars-cov-2 virus, or popularly called the Coronavirus or COVID-19, many have been forced to use technological means as, perhaps, the only way out to continue with their daily tasks, and thus ensure, in times of crisis, the support for their families.

On the other hand, due to, many times, the lack of skills and habits with such resources, Internet users have become easy targets for cybercriminals, who take advantage of the moment and of their naivety to apply their techniques and thus ensure success in their criminal enterprise.

Starting from this premise, the subject of cybersecurity began to be more explored and even valued by those who never worried about it. Thus, security protocols had to be created with more rigor, since data integrity became paramount to ensure the full and safe operation of online services.

When it comes to children and teenagers, perhaps more important than cybersecurity protocols is to control the amount of time they spend using the Internet, since their exposure can bring about several harmful consequences, which may even irreversibly affect their mental health.

We conclude then that caution and safety rules should always be observed before diving so deeply into the virtual world, that is, cyberspace, since besides the many benefits it can provide, we have the harms it can bring to life, whether related to physical or psychological integrity.

REFERENCES

[1] ABUKARI, Arnold Mashud; BANKAS, Edem Kwedzo. *Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond*. Recovered in 18 de july, 2020, from https://www.researchgate.net/publication/341098664_Some_Cyber_Security_Hygienic_Protocols_For_Teleworkers_In_Covid-19_Pandemic_Period_And_Beyond.

[2] AHMAD, Tabrez. *Corona Virus (Covid-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. Recovered in 12 july, 2020, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3568830.

[3] AVAST. *O guia essencial sobre phishing: Como funciona e como se proteger*. Recovered in 12 de july, 2020, from https://www.avast.com/pt-br/c-phishing#topic-1.

[4] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Recovered in 11 july, 2020, from http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

[5] DESLANDES, Suely Ferreira; COUTINHO, Tiago. *O uso intensivo da internet por crianças e adolescentes no*

contexto da Covid-19 e os riscos para violências autoinflingidas. Recovered in 17 july, 2020, from https://www.scielo.br/scielo.php?pid=S1413-81232020006702479&script=sci_arttext.

[6] DOMINGUES, Vinícius. *Em tempos de pandemia, é preciso ter muita atenção com os cibercrimes*. Recovered in 11 july, 2020, from https://www.conjur.com.br/2020-mai-13/domingues-cibercrimes-tempos-pandemia.

[7] GONÇALVES, Victor Minarini. *VITIMOLOGIA: CONCEITUAÇÃO E APLICABILIDADE*. Recovered in 17 de july, 2020, from https://jus.com.br/artigos/36073/vitimologia-conceituacao-e-aplicabilidade.

[8] GOUVEIA, Luis Borges. *Covid-19 e Desafios para a Cibersegurança num Tempo pós-Pandemia*. Recovered in 17 july, 2020, from https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20july%202020%204%C2%AAvers%C3%A3o.pdf

[9] JESUS, Helder Fialho de. *Ciberespaço e Mundo Físico – As Duas Faces da Mesma Moeda*. Recovered in 19 july, 2020, from https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/IDN%20brief%209%20july%202020%204%C2%AAvers%C3%A3o.pdf

[10] KASPERSKY. *O que é ransomware?*. Recovered in 11 july, 2020, from https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware.

[11] MALAVÉ, Mayra Malavé. *O papel das redes sociais durante a pandemia*. Recovered in 11 july, 2020, from http://www.iff.fiocruz.br/index.php/8-noticias/675-papel-redes-sociais.

[12] NAIDOO, Rennie. *A multi-level influence model of COVID-19 themed cybercrime*. Recovered in 09 july, 2020, from https://orsociety.tandfonline.com/doi/full/10.1080/0960085X.2020.1771222.

[13] RAHAL, Carla; TURRINI, Janaina; FIORESE, Urbano; FURTADO, Felipe. *Crimes digitais e prevenção em época de pandemia*. Recovered in 12 july, 2020, from https://cryptoid.com.br/banco-de-noticias/crimes-digitais-e-prevencao-em-epoca-de-pandemia/.

[14] RIBEIRO, Gustavo Lins. *Medo Global. Boletim n. 5. Cientistas sociais e o coronavírus*. Anpocs. Recovered in 14 july, 2020, from http://www.anpocs.com/index.php/ciencias-sociais/destaques/2311-boletim-n-3.

[15] RODRIGUES, Renato. *Brasil é líder em empresas atacadas por ransomware na epidemia*. Recovered in 11 july, 2020, from https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527/.

International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-8, Issue-9; Sep, 2021
Journal Home Page Available: https://ijaers.com/
Article DOI: https://dx.doi.org/10.22161/ijaers.89.7

Threats and vulnerabilities associated with cybercrime with children and adolescents

Ameaças e vulnerabilidades associadas aos cibercrimes com crianças e adolescentes

Thiago José Ximenes Machado[1], Luís Borges Gouveia[2]

[1]Tecnólogo em Processamento de Dados; Bacharel em Direito; Pós-Graduado em: Rede de Computadores; Perícia Digital e Computação Forense (em andamento); Direito Penal e Processual Penal; Criminologia; Ciências Criminais; Política e Gestão em Segurança Pública; Direito Eletrônico (em andamento); Mestre em Criminologia e Doutorando/PhD em Ciência da Informação – Universidade Fernando Pessoa – Cidade do Porto (Portugal).
[2]Luis Borges Gouveia. Concluiu o Título Acadêmico de Agregado em 2010 pela Universidade de Aveiro e o Doutoramento em Ciências da Computação em 2002 pela Lancaster University (Reino Unido) e o Mestrado em Engenharia Electrotécnica e de Computadores em 1995 pela Universidade do Porto. Professor Catedrático da Universidade Fernando Pessoa.

Received: 16 Jul 2021,
Received in revised form: 25 Aug 2021,
Accepted: 04 Sep 2021,
Available online: 14 Sep 2021

Keywords— ***Internet, Children and adolescents, Cybercrimes, Vulnerable, Criminal types.***

Abstract— *This scientific initiation article will address the main threats found in the virtual world, especially those that tend to reach children and adolescents, who currently use the tools available on the internet continuously and devolved. We will also show the penal aspects established in Brazilian law, as well as a statistic of the number of crimes of this kind practiced throughout the year 2018 and in the first months of 2019, making an analysis of growth or reduction of these. At the end of the day we will reflect, based on the studies and data collected, on the dangers that this public is considered vulnerable, when they navigate the world wide computer network without control and without the necessary expertise to detect a possible crime.*

Resumo— *Este artigo de iniciação científica irá abordar as principais ameaças encontradas no mundo virtual, em especial aquelas que tendem a atingir crianças e adolescentes, que, na atualidade, utilizam de forma contínua e desvigiadas as ferramentas disponíveis na internet. Mostraremos, também, os aspectos penais dispostos na lei brasileira, assim como uma estatística do número de delitos dessa espécie praticados em todo o ano de 2018 e nos primeiros meses de 2019, fazendo uma análise de crescimento ou de redução destes. Ao final faremos uma reflexão, com base nos estudos e dados colhidos, sobre os perigos a que estão sujeitos, esse público considerado vulnerável, quando navegam pela rede mundial de computadores sem controle e sem a expertise necessária para detectar um possível delito.*

Palavras-Chave— ***Internet, Crianças e adolescentes, Cibercrimes, Vulnerabilidade, Tipos penais.***

I. INTRODUÇÃO

Na era digital, cada vez mais presente na vida cotidiana, os aparelhos de televisão, de rádio, e até mesmo a velha e conhecida agenda, foi dando lugar a um equipamento, que se tornou, praticamente, indispensável nos lares atuais, o computador. Por outro lado, os smarts phones também se tornaram acessórios da vida das pessoas, já que estes fazem o papel de computadores portáteis.

Começaremos falando sobre a vulnerabilidade que perfaz o público infanto-juvenil quando, sem nenhum temor, exploram vários ambientes virtuais disponíveis na rede mundial de computadores, acreditam em que não correm perigo algum.

Em um segundo momento, mostraremos,de forma conceitual, as ameaças mais conhecidas do mundo virtual, e que vêm fazendo muitas vítimas, em especial aquelas na faixa etária que englobam as crianças e os adolescentes.

Em continuidade, falaremos quais potenciais risco de se concretizarem as ameaças existentes no uso desenfreado da internet, em especial, por aqueles que estão em pleno desenvolvimento psicológico e, por isso, são considerados vítimas perfeitas de cibercrimes.

Logo após, descreveremos os delitos que estão tipificados na legislação especial criminal brasileira, hora denominada Estatuto da Criança e do Adolescente, que por sigla ECA, trazendo as condutas consideradas delituosas e suas respectivas sanções.

Com base nos dados estatísticos, no item quatro, faremos a análise comparativa entre os meses de janeiro de 2018 a abril de 2019, para entender o fenômeno criminal, e suas tendências de crescimento ou diminuição, na medida em que as pessoas acessam o cenário virtual, e acabam por serem vítimas, já que muitas vezes desconhecem ou não se preocupam com os perigos que estão por trás dos ecrãs.

Em seguida, iremos mostrar alguns casos registrados no banco de dados da polícia judiciária, fazendo análise e, posteriormente, reflexões das vulnerabilidades e dos modos de execuções dos ditos cibercrimes.

Finalmente, será trazida uma reflexão sobre os perigos atuais e iminentes a que estão sujeitos, aqueles que consideramos como público vulnerável em decorrência de vários fatores que foram mostrados no transcorrer do artigo.

II. MÉTODO

A metodologia aplicada foi qualitativa, caracterizada pela análise de outros artigos, documentos oficiais que trazem informações relacionadas ao tema abordado, bem como, análise de dados extraídos de sistema interno da polícia civil.

A partir dessasinformações, extremamente relevantes, podemos perceber o qual vulnerável é o público infanto juvenil, que por vezes, acreditam ter a expertise para navegar no mundo virtual sem que sejam alvos dos algozes cibercriminosos.

O estudo contou com um volume considerável de artigos científicos, de forma que de cada um foi extraído o conhecimento necessário para desenvolver informações relevantes para compor nossa pesquisa científica.

A partir do conteúdo explorado, extraímos diversas informações que vão desde a vulnerabilidade infanto-juvenil, perpassando pelas ameaças associadas, especialmente, as crianças e aos adolescentes, incluindo a probabilidade dessas ameaças se tornarem fato criminoso, e, finalmente, análises de dados e reflexões sobre o tema.

Por fim, mostramos a conclusão que foi tirada após o estudo e que certamente contribuirá para a sociedade em geral, uma vez que a conectividade, atualmente, atinge grande parte da população mundial, independente da classe social, principalmente, as crianças e os adolescente que estão a cada dia mais envolvidos com a era tecnológica.

III. VULNERABILIDADE INFANTO-JUVENIL

É de suma importância ressaltar que os sujeitos passivos da vulnerabilidade tratada neste capítulo têm idades que foram pré-definidas no artigo 2° do ECA[1] (Estatuto da Criança e do Adolescente), que traz "*Art. 2° Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade*". Ressaltando ainda que o artigo 3° do mesmo estatuto traz os direitos fundamentais que derrogam esse público, assim descrevendo,

> *Art. 3° A criança e o adolescente gozam de todos os direitos fundamentais inerentes à pessoa humana, sem prejuízo da proteção integral de que trata esta Lei, assegurando-se-lhes, por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade.*

O fluxo de informações proporcionado pela internet é imensurável, e tendo em vista essa facilidade é que os algozes agem nesse ambiente virtual, trazendo riscos, em especial, para o público infanto-juvenil, pois

[1]BRASIL. Lei nº 8.609, de 13 de julho de 1990. Recuperado em 25 de abril de 2018, from http://www.planalto.gov.br/ccivil_03/leis/L8069.htm.

estes tendem a explorar o cyber ambiente de maneira destemida e sem nenhuma forma de cuidado, o que faz com que, muitas vezes, eles contribuam com sua própria vitimização.

Os criminosos que agem no mundo virtual e que comentem delitos contra as crianças e os adolescentes se prevalecem de alguns fatores que fazem parte da personalidade desse público, quais sejam: a autoconfiança de que nada de ruim acontecerá; o prazer de desafiar os pais; a sensação de terem esperteza suficiente para navegar na internet; busca por aventuras e por experiências novas; a exposição da vida pessoal; dentre outros[2].

Este público se torna mais vulnerável, na medida em que os seus pais ou responsáveis legais, perdem o controle e deixam de monitorar o acesso à internet de seus filhos, que, em razão da falta de maturidade e da imensidão de conteúdo trazido pelo mundo virtual, acabam atraídos pelos criminosos que se utilizam desse cenário para prática de delitos.

Devido à gama de informações fornecidas pela própria vítima, os abusadores criam a melhor estratégia para atraí-las, seja criando perfis de pessoas da mesma faixa etária, ou verificando as preferências de sua presa para então realizar uma aproximação.

Quando estamos tratando, exclusivamente, do público adolescente que está em pleno desenvolvimento da sexualidade, temos que estes se tornam ainda mais vulneráveis, devido a esta fase de suas vidas, ou seja, a puberdade. Além disso, destacamos que,por falta de uma melhor orientação, os de classes mais baixas são os mais atingidos[3].

Constatamos assim que os fatores de vulnerabilidade que existem, em especial, nos infanto-juvenis, se dão por fatores biológicos, sociais e comportamentais. Porém a falta de orientação, tanto por parte dos pais como do poder público, tende a fortalecer a facilidade de ataque a estas vítimas, em se tratando de um ambiente virtual fértil para a prática de delitos.

VULNERABILIDADES	SIGNIFICADO
Relativo à idade	O acesso às ferramentas tecnológicas com idades cada vez mais baixas.
Relativo à falta de preparação	Não maioria dos casos, crianças e adolescentes ingressam no mundo virtual sem antes ter uma orientação.
Relativo à falta de monitoramento	Os pais ou responsáveis legais, muitas vezes, não se preocupam em monitorar os acessos dos filhos.
Relativo à falta de políticas de segurança específicas	O governo não se preocupa em fazer campanhas de prevenções para os cibercrimes, e muito menos, alertas para o acesso irrestrito de crianças e de adolescente, mostrando os riscos reais.
Relativo ao vício digital	Nos dias atuais, crianças e adolescentes trocaram as brincadeiras tradicionais pelos equipamentos eletrônicos, em especial smartphones e computadores.

IV. AMEAÇAS CIBERNÉTICAS ASSOCIADAS ÀS CRIANÇAS E AOS ADOLESCENTES

As tecnologias vêm despertando o interesse das pessoas há alguns anos, todavianão podemos negar que a maior afinidade e a facilidade em lidar com essas inovações vêm das crianças e dos adolescentes.

A facilidade de desenvolver as atividades diárias, seja no âmbito educacional, profissional ou ainda para o momento de entretenimento, utilizando as ferramentas tecnológicas disponíveis na internet, vem crescendo a cada dia, apesar de ainda ter certa rejeição do público com maiores idades.

Neste cenário, em que os pais, não raras vezes, perderam o que há de mais importante na sua relação com os filhos, ou seja, o diálogo, o computador vem se tornando o melhor e mais fiel amigo das crianças e dos jovens, fazendo com que estes exponham todos seus

[2]SILVA, Rosane Leal da; Veronese, Josiane Rose Petry. *Os crimes sexuais contra criança e adolescente no ambiente virtual*. Recuperado em 19 de abril, 2019, from http://www.ambito-juridico.com.br/site/index.php?artigo_id=6634&n_link=revista_artigos_leitura.

[3]BRETAN, Maria Emilia Accioli Nobre, VIOLÊNCIA SEXUAL CONTRA CRIANÇAS E ADOLESCENTES MEDIADA PELA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: ELEMENTOS PARA PREVENÇÃO VITIMAL. Recuperado em 25 de abril, 2019, from https://www.teses.usp.br/teses/disponiveis/2/2136/tde-22042013-111456/publico/TESE_COMPLETA_MARIA_EMILIA_A_N_BRETAN_FD_USP2012.pdf.

sentimentosaos amigos virtuais[4].

Dentre os diversos delitos que podem ser praticados contra os sujeitos passivos em destaque no presente artigo, temos aqueles ditos mais gravosos, pois lesam bem jurídico denominado dignidade sexual. Assim, denominamos os crimes desta natureza como pedofilia infanto-juvenil, já que as vítimas desse ato criminoso podem ser tanto crianças como adolescentes.

É importante conhecermos o conceito dado pela Organização Mundial de Saúde em se tratando do termo pedofilia, que segundo esta é a "Preferência sexual por crianças, quer se tratem de meninos, meninas ou de crianças de um ou do outro sexo, geralmente pré-púberes ou no início da puberdade[5]". Assim, podemos dizer que se trata de um desvio de conduta sexual (parafilia), ou seja, o criminoso possui uma perversão sexual, caracterizadas por fantasias, anseios ou atividades incomuns que trazem sofrimento clinicamente significativo ou propiciando comportamentos sociais e ocupacionais inadequados, tendo como objeto de desejo a criança.

Não se pode negar que a facilidade encontrada por esses pedófilos, em conseguir se aproximar das vítimas mais vulneráveis, teve um crescimento significativo após a explosão das tecnologias que estão diretamente ligadas à internet, justificando assim a criação de novos tipos penais, que foram acrescidos no Estatuto da Criança e do Adolescente, os quais estão voltados aos delitos praticados na rede mundial de computadores.

No Brasil, discute-se a necessidade de uma legislação ainda mais completa sobre os crimes praticados por meios da internet, todavia existem doutrinas que divergem deste pensamento, pois acreditam em que haverá um excesso de normas, sendo tais imposições desnecessárias[6].

Por outro lado, as ameaças crescem a cada dia, tendo em vista uma combinação perfeita para os criminosos, a qual se dácom facilidade que os meios virtuais proporcionam,juntamente com a dificuldade de localização dos criminosos, a falta de uma legislação mais específicae o tratamento brando que a normal penal traz, ao fazer o enquadramento em legislação penal.

De acordo com a Organização dos Estados Americanos (OEA), por meio de sua agência especializada em crianças e adolescentes, o Instituto Interamericano da Criança (IIN)[7], foi divulgada uma publicação sobre as principais ameaças que podem atingir crianças e adolescentes, das quais podemos citar: abuso sexual de crianças e de adolescentes na Internet; cyberbullying; exposição a conteúdos inapropriados; grooming (estratégia para ganhar confiança de criança e adolescente, usada para fins libidinosos); happy slapping (uma forma de cyber-violência, em que é filmado e depois postado na internet, o ataque humilhante); sexting (forma de pressionar crianças e adolescentes a enviar fotos de teor sexual); sextortion (extorquir uma pessoa, com ameaças de enviar suas fotos íntimas) etc.

Inferimos, então, que as ameaças trazidas pelo uso de tecnologias ligadas à internet podem ter as mais diversas variações, que pode culminar com delitos menos graves como injúria, calúnia e difamação, até os mais gravosos, que são os praticados contra a vida e a dignidade sexual das crianças e adolescentes.

V. OS RISCOS DE CONCRETIZAÇÃO DAS AMEAÇAS EM FACE À VULNERABILIDADE INFANTO-JUVENIL

A vulnerabilidade nos reporta à ideia de sensibilidade ou de fraqueza relacionada à determinada área, fazendo com que aumente a possibilidade de ser afetado de alguma forma. E, em se tratando de mundo digital, este fator negativo pode interferir das mais variadas maneiras, na saúde física e, principalmente, mental das crianças e dos adolescentes[8].

Com advento das redes sociais, os riscos aumentaram significativamente, tendo em vista que agora há uma interação "real", crescendo assim as ameaças

[4]EISENSTEIN E, Estefenon S. *Computador: ponte social ou abuso virtual?*. Adolesc Saude. 2006;3(3):57-60. Recuperado em 09 de abril, 2019, from http://adolescenciaesaude.com/detalhe_artigo.asp?id=136.

[5] Conceito extraído da Classificação Internacional de Doenças (CID) da Organização Mundial de Saúde (OMS). Recuperado em 25 de abril, 2019, from http://cid10.bancodesaude.com.br/cid-10-f/f654/pedofilia.

[6]SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallas Tomaz. RELAÇÕES JURÍDICAS VIRTUAIS: ANÁLISE DE CRIMES COMETIDOS POR MEIO DO USO DA INTERNET. Recuperado em 25 de abril, 2019, from http://egov.ufsc.br/portal/sites/default/files/3952-21333-1-pb.pdf.

[7] MENDOZA, Miguel Ángel. *Os 10 principais riscos na Internet para crianças e adolescentes*. Recuperado em 03 de maio, 2020, from https://www.welivesecurity.com/br/2018/05/21/principais-riscos-na-internet-para-criancas-e-adolescentes/.

[8]FONSECA, Franciele Fagundes; SENA, Ramony Kris R.; SANTOS, Rocky Lane A. dos; ORLENE, Veloso Dias; COSTA, Simone de Melo. *As vulnerabilidades na infância e adolescência e as políticas públicas brasileiras deintervenção*. Recuperado em 30 de março, 2020, fromhttps://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-05822013000200019.

virtuais, deixando a vulnerabilidade do público infanto-juvenil ainda mais evidente, pois, estão em fase de desenvolvimento psicológico, o que, muitas vezes, contribui para a ação dos algozes.

Podemos fazer uma reflexão, analisando o posicionamento de Pereira (2015),

> Ao permitir a entrada de menores de idade em sites cujo objetivo é a interação social através da publicação de atividades rotineiras e exposição de fotos, acontece a superexposição da criança ou adolescente que inconscientemente atrai diversos outros perigos para si, mostrando-se vulnerável a atuações de marketing, de criminosos ou até mesmo da espionagem da sociedade.

Os posts publicados nas redes sociais, embora pareça algo norma e inofensivo, podem ser um forte fator de risco para os menores de idade, já que, muitas vezes, os pais, de maneira inconsciente, colocam fotos de nudez ou que identifique sua morada, criando assim riscos, seja com maior ou menor possibilidade de ocorrência.

Devido ao grande bombardeio de informações e conceitos que são impostos pela sociedade, podemos verificar que uma simples postagem de um adolescente, por exemplo, pode gerar uma série de críticas, transformando-se assim no conhecido e venenoso ciberbullying, o qual, na maioria das vezes, atinge o psicológico de forma avassaladora[9].

A pedofilia infantil, podemos citar, também, como um risco iminente de ocorrer, caso fotos de nudez ou sensuais caiam nas mãos de pedófilos. Esses têm a seu favor a possibilidade de propagação de tais imagens, nas denominada deep web, ou seja, uma rede obscura na qual ocorrem os mais variados delitos na internet.

Outro problema muito presente no acesso desse público sem expertise é que esta inexperiência é aproveitada pelos criminosos, agindo de forma a convencer, em especial, as crianças a fornecer dados relacionados a cartões de créditos de seus pais. Para isso, criam personagens que irão interagir com essas crianças, com objetivo de obter tais informações.

O ciberespaço é considerado ambivalente, ou seja, potencialidade e risco são bem definidos, assim, a preservação dos direitos fica iminentemente comprometida. Este acesso fica ainda mais perigoso, quando as tecnologias ligadas à internet se tornam rotina na vida de crianças e de adolescentes, fazendo deste, muitas vezes, uma fuga dos problemas do mundo real. Todaviaestes acabam por ingressar em um perigoso mundo virtual, em queas situações desastrosas podem tornar a vida desses vulneráveis ainda mais devastada[10].

Inferimos então que, por se encontrarem em processo de desenvolvimento físico e psíquico, crianças e adolescente não conseguem ter a percepção dos riscos em potencial os quais estão expostos, sendo estes os mais variáveis, como por exemplo, ciberbullying, crimes contra honra, aliciamento para fins sexuais,pedofilia e muitos outros.

VI. INSERÇÕES E ALTERAÇÕES DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE POR MEIO DA LEI 11.829/08

A lei 11.829/08 traz alterações nos artigos 240 e 241 da lei 8.069/90 (Estatuto da Criança e do Adolescente - ECA), assim como inserções de novos artigos, quais sejam 241-A, 241-B, 241-C, 241-D e 241-E,que vem a aprimorar o combate à produção, à venda e à distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet[11].

No artigo 240 e seus parágrafos e incisos, o ECA vem a discorrer sobre as condutas tipificadas como crimes e suas respectivas sanções para aquele que dirigi, filma, produz ou fotografa, cenas de sexo explícito ou pornográfico, que tenha a participação de criança ou de

[9] FEUSER, Bruna Ceccone; PAVEI, Fernando; NETO, Pedro Zilli; ZOMER, Ramirez; PAVEI, Rodrigo. *A VULNERABILIDADE DA CRIANÇA E DO ADOLESCENTE NAS REDES SOCIAIS: NECESSÁRIA CAUTELA PARA A SEGURANÇA DO PÚBLICO INFANTO-JUVENIL*. Recuperado em 01 de maio, 2020, from http://periodicos.unibave.net/index.php/constituicaoejustica/article/view/115.

[10] SOUZA, Dercia Antunes de; OLIVEIRA, Joyce Alessandra de Moraes. *USO DE TECNOLOGIAS DIGITAIS POR CRIANÇAS E ADOLESCENTES: POTENCIAIS AMEAÇAS EM SEUS INTER-RELACIONAMENTOS*. Recuperado em 01 de maio, 2020, from https://www.aedb.br/seget/arquivos/artigos16/952473.pdf

[11] MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático: A especial vulnerabilidade das crianças e dos adolescentes*. Recuperado em 13 de maio, 2019, from https://bdigital.ufp.pt/handle/10284/6089.

adolescente. O parágrafo primeiro traz o delito por equiparação, ou seja, iráincorrer nas mesmas penas, quais sejam, de 4 (quatro) a 8 (oito) anos de reclusão em conjunto com multa, o sujeito que agencia, facilita, coage ou intermedia esse envolvimento de menores. E o segundo e último parágrafo vem a trazer as causas aumento de pena, quando o crime for cometido por aqueles agentes que, devido a sua profissão ou grau de parentesco, possuem maior proximidade com vítima.

O artigo 241 da lei supracitada apresenta punição semelhando àqueles que praticam as condutas de vender (inclusive utilizando a internet) ou expor o material pornográfico no qual há envolvimento de crianças ou de adolescente em cena de sexo explícito ou pornográfica, aplicando, inclusive, as mesmas penas descritas no artigo 240, quais sejam, 4 (quatro) a 8 (oito) anos de reclusão associadas com multa.

Com a inserção do artigo 241-A, os legisladores tiveram a expertise direcionada, principalmente, aos meios virtuais de comunicação, em especial a internet, tendo em vista o crescimento de sua utilizaçãodesde o final dosanos 90,e que vem aumentando a cada dia. Assim,a lei traz uma punição também aos os que praticarem a conduta de transmitir, disponibilizar, publicar, divulgar etc., fotos, vídeos e outros materiais que contenham cena de sexo explícito ou de pornografia com crianças e adolescente. Vale destacarque será aplicada a mesmasanção ao responsável legal do website, caso este seja notificado oficialmente, e não desative o acesso ao conteúdo proibido, que é reclusão de 3 (três) a 6 (seis) anos, cumulado com multa.

Seguindo para o artigo 241-B, não foi esquecidoaquele que adquirir, possuir ou armazenar (em computadores, celulares e outros), os materiais ilícitostrazidospelos artigos anteriores, podendo ter pena de 1 (um) a 4 (quatro) anos de reclusão e multa. No parágrafo primeiro, o legislador entendeu que a pena deve ser reduzida de dois terços, caso a quantidade de material encontrado seja pequena. E o parágrafo seguinte, dispõeda atipicidade do fato, quando a posse ou o armazenamento desse conteúdofor feita com a finalidade de comunicar as autoridades competentes. Todavia existe um rol de agentes que podem praticar a conduta de possuir ou armazenar, quais sejam, agente público no exercício de suas funções, membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo,ainda faz parte destes, orepresentante legal e os funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário. E finalmente temos a solicitação para que os agentes elencados anteriormente mantenham o sigilo para que a investigação tenha êxito.

O artigo 241-C da lei em comento vem a punir a adulteração, a montagem ou a modificação de imagens, utilizando-se de todo e qualquer meio de produção que envolva crianças ou adolescente em cenas de pornografia ou sexo explícito, tendo uma reprimenda que vai de 1 (um) a 3 (três) anos de reclusão e multa.Em seu parágrafo único,traz as condutas equiparadas, as quais terão as mesmas punições, para quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do artigo 241-C.

Com pena semelhante ao artigo anterior, o artigo 241-D vem a punir o ato de "Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso". Logo, é de suma importância se faz entender o verdadeiro conceito de ato libidinoso, para tal nos aproveitaremos das palavras de Rogério Sanches[12] (2016, p. 213 – 214), que assim se manifesta:

> A expressão "ato libidinoso" é bastante ampla, porosa e, se não interpretada com cautela, pode culminar em séria injustiça, como já registrada pela nossa jurisprudência quando os Tribunais subsumiam ao tipo, o simples beijo lascivo. Deve o aplicador aquilatar o caso concreto e concluir que o ato praticado foi capaz de ferir ou não a dignidade sexual da vítima com a mesma intensidade de uma conjunção carnal. Como exemplo citamos o coito *per anun*, *inter femora*, a *fellatio*, o *cunnilingus*, ou ainda a associação da *fellatio* e o *cunnilingus*, a cópula axiliar, entre os seios, vulvar etc.

As condutas equiparadas vêm dispostas no parágrafo único do mesmo artigo, a qual será aplicada a mesma sanção para aquele que facilitar ou induzir criança

[12] SANCHES, Rogério Cunha. *CÓDIGO PENAL para concursos. 9ª ed. Revista, ampliada e atualizada*. Editora: Jus Podivm, 2016.

a ter acesso a material contendo cena de sexo explícito ou pornográfica com a finalidade de com ela praticar ato libidinoso, ou ainda, praticar as condutas descritas no artigo 241-D com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita, inclusive por meios virtuais.

No último artigo, qual seja o 241-E, que foi incluído pela lei 11.829/08 nos depararemos com a explicação relacionada à expressão "cena de sexo explícito ou pornográfica", a qual na sua literalidade traz "compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais".

Induzimos assim que a legislação especial se preocupou com os delitos praticados, em especial por meio de ferramentas disponibilizadas na internet, apesar de muitos estudiosos do direito penal acharem que as sanções ainda são muito brandas, tendo em vista o grau de reprovabilidade da conduta e o dano que esta pode vir a causar, não só à vítima imediata, como àqueles que fazem parte de sua vida.

VII. ESTATÍSTICA DE REGISTRADOS DOS CIBERCRIMES ENVOLVENDO CRIANÇAS E ADOLESCENTES PRATICADOS NO ESTADO DO PARÁ ENTRE JANEIRO DE 2018 E ABRIL DE 2019

Com base em dados que foram colhidos a partir do sistema de registro de ocorrências e procedimento da polícia judiciária do Estado do Pará, denominado SISP (Sistema Integrado de Segurança Pública), analisaremos os números apresentados de janeiro de 2018 a abril de 2019, relacionados à comunicação de crimes praticados contra crianças e adolescentes por meio da internet.

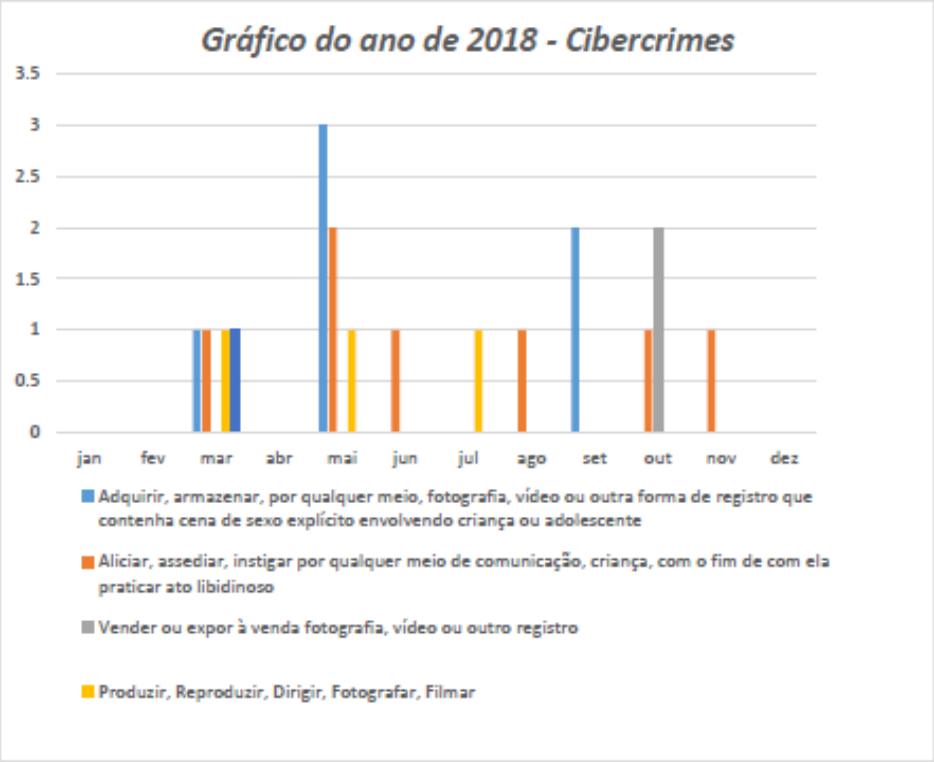


Fig.1 - Dados do sistema da polícia civil do Estado do Pará

O gráfico mostra os dados do ano de 2018, dentre os quais selecionamos os diretamente relacionados à dignidade sexual das crianças e dos adolescentes, e que são praticados por meios de ferramentas computacionais e foram registrados nas delegacias especializadas em crimes tecnológicos.

Durante o ano de 2018, tivemos, no Estado do Pará, ocorrência do delito somente nos meses de março (1 ocorrência), maio (3 ocorrências) e setembro (2

ocorrências) da prática do crime de adquirir, de armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito envolvendo criança ou adolescente, descrito no artigo 241-B do ECA.

Já nos meses de março (1 ocorrência), maio (2 ocorrências), junho (1 ocorrência), agosto (1 ocorrência), outubro (1 ocorrência) e novembro (1 ocorrência) de 2018, foram registradas a prática da ação criminosa descrita no artigo 241-D do ECA, que trata de aliciar, de assediar, de instigar por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso. Estes praticados, principalmente, por meios de redes sociais e de aplicativos de mensagens instantâneas.

Foi registrado somente no mês de outubro (2 ocorrências) de 2018, o delito de vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente, disposto no artigo 241 do ECA.

Em se tratando de crime voltado a produzir, reproduzir, dirigir, fotografar, filmar público em estudo, tivemos registros nos meses de março (1 ocorrência), maio (1 ocorrência) e julho (1 ocorrência).

O delito que teve mesmo ocorrência no ano de 2018 foi o de simular a participação de criança ou de adolescente em cena de sexo explícito por meio de adulteração, de montagem ou de modificação de fotografia, vídeo ou qualquer outra forma de representação visual, onde somente foi registrado 1 (uma) prática no mês de março.

Partindo agora para uma análise dos quartos primeiros meses do ano de 2019, tendo em mente os mesmos delitos comentados anteriormente, foi reproduzido um gráfico que demonstrará as respectivas ocorrências.

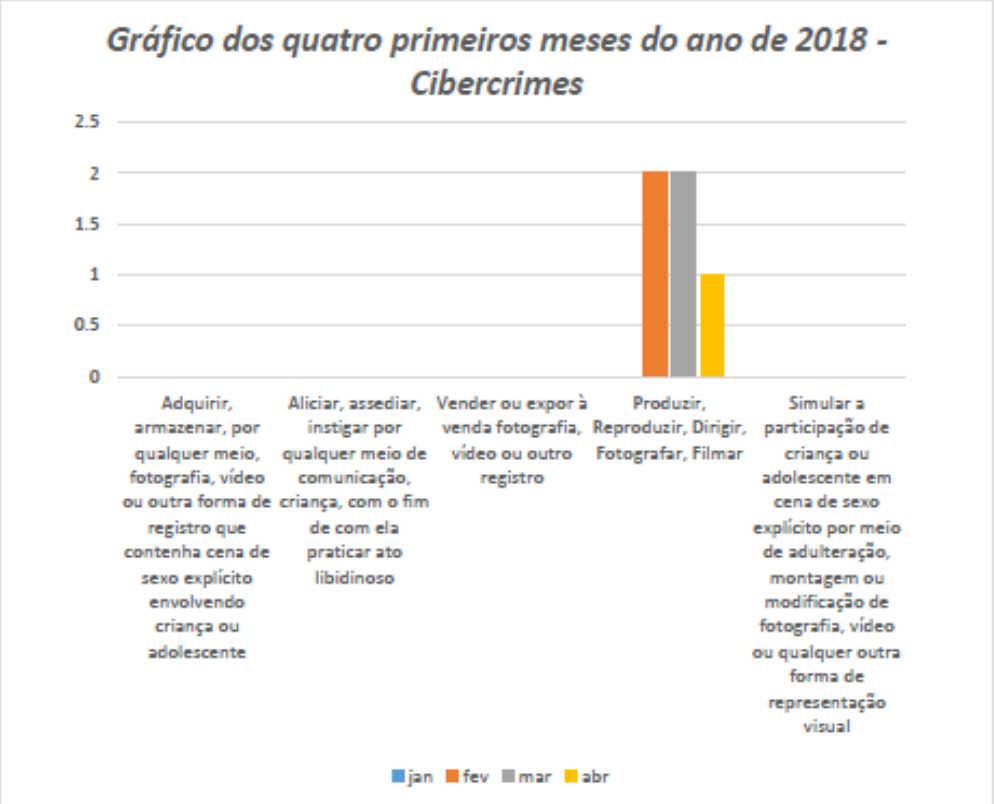


Fig.2 - Dados do sistema da polícia civil do Estado do Pará

Continuando a análise, podemos observar, claramente, que houve uma queda de quatro dos cincos delitos mostrados, em que somente ocorreu o aumento da prática do crime no delito de produzir, de reproduzir, de dirigir, de fotografar, de filmar crianças e adolescente em cena de sexo explícito ou pornográfica. Neste foram contabilizadas 5 ocorrências, sendo 2 (duas) no mês de fevereiro, 2 (duas) no mês de março e 1 (uma) no mês de abril.

Vale ressaltar que o número relativamente baixo de cibercrimes praticados contra crianças ou adolescente, se dá por um fenômeno denominado cifra escura, a qual ocorre quando os delitos não chegam ao conhecimento das autoridades, seja por medo do criminoso, ou pelo fato de achar que a justiça ficará inerte e o autor não será punido.

VIII. REFLEXÃO DOS CUIDADOS DO ACESSO À INTERNET FEITO POR CRIANÇAS E ADOLESCENTES

Atualmente, sabemos que a internet tem como realidade um vasto terreno nocivo, e que devido ao grande número de programas utilizados como mecanismo para proteção dos usuários, os criminosos especializados nos ataques virtuais conseguem camuflar as suas ações, passando por cima das barreiras protecionais, já que a obscuridade e a extensão espacial proporcionada pelo acesso torna a segurança difícil ou até mesmo impossível de ser combatida de forma absoluta.

Partindo da ideia de que as crianças e os adolescentes acessam a rede mundial de computadores sem nenhum temor, o melhor caminho seria, de fato, a orientação no uso desenfreado, assim como mostrar os riscos e ensinar a identificá-los, fazendo com que sejam criados por esses usuários, os seus próprios mecanismos de defesa. Tendo em vista que, na atualidade, a internet e seus perigos são incontornáveis, a prevenção se mostra mais eficiente do que a proibição[13].

Um aspecto extremamente relevante, que explica o porquê as crianças e os adolescentes mergulham na imensidade dos espaços virtuais, diz respeito à sensação de controle que estes exercem sobre si mesmos. Assim, acreditam em que não há nada de mais em publicar, por exemplo, uma foto expondo partes do seu corpo ou até mesmo sexualizando. Todavia esse tipo de postagem atrai os pedófilos e, com base nas informações colhidas, tem condições de se aproximar da vítima e obter sucesso no seu intento.

Outro aspecto importante é que muitas imagens, vídeos e publicações inadequadas, podem influenciar de maneira negativa na formação de crianças ou de jovens, em que a visualização destes conteúdos pode ser internalizada como prática de condutas normais, como exemplo, os vídeos de violência ou até mesmo de pornografia envolvendo práticas sexuais com crianças, animais, dentre outros.

[13] MONTEIRO, Ana Francisca Cunha. A INTERNET NA VIDA DAS CRIANÇAS: COMO LIDAR COM PERIGOS E OPORTUNIDADES. Recuperado em 25 de junho, 2019, fromencurtador.com.br/abqKT.

Como tudo na vida, temos dois lados, o bom e o ruim. Assim acontece com a internet, que se mostra uma ferramenta com vasto conteúdo valoroso, basta que seja explorada com responsabilidade e as devidas orientações daquele que possuem mais expertises no assunto, fazendo assim com que as chances de ser uma vítima em potencial reduzam drasticamente.

Muitos países do mundo vêm investindo na criação de mecanismo de proteção online para crianças e adolescentes, com objetivo de coibir a exposição destes. Todavia sabemos o quão difícil é ter esse controle, pois, apesar das redes sociais não autorizem menores de idade criar perfis, isso é facilmente burlado.

O Brasil ainda se mostra muito carente com relação as legislações que tratam sobre os crimes praticados por meios virtuais, apesar de termos lei que dispõe sobre o tema, estas, ao nosso ver,devem evoluir muito. Por outro lado, nos parece que seria necessária a criação de normas de proteção, quando se tratar do acesso de menores à rede mundial de computadores, incluindo responsabilização aos pais omissos[14].

Findamos assim, com ideia de que a melhor maneira de se resguardar contra os diversos ataques advindos da internet é criarmos técnicas de prevenção, nas quais podemos orientar nossas crianças e adolescente, para que estas possam explorar o mundo virtual de forma saudável e contributiva para seu desenvolvimento psíquico intelectual.

IX. CONSIDERAÇÕES FINAIS

Não podemos negar que a criação e a evolução da rede mundial de computadores nos proporcionaram inúmeras facilidades e comodidade que abrangem, praticamente, todas as áreas e atividades de nossas vidas. Assim, milhares de pessoas são atraídas e adentram este mundo virtual, porém de grande e considerável efeito no mundo real.

As crianças ganharam uma nova ferramenta de aprendizagem, facilitando e inovando a forma de aprender. Pois, com a gama de informações encontradas em sites educativos, ficou muito mais fácil obter informações relacionadas ao mundo acadêmico.

Os adolescentes, por sua vez, encontraram na internet uma nova forma de se relacionar com o mundo e,

[14] PEREIRA, Marília do Nascimento. *A SUPEREXPOSIÇÃO DE CRIANÇAS E ADOLESCENTES NAS REDES SOCIAIS: necessária cautela no uso das novas tecnologias para a formação de identidade*. Recuperado em 10 de maio, 2020, from http://coral.ufsm.br/congressodireito/anais/2015/6-14.pdf.

assim, descobriram um universo no qual suas opiniões e paixões podem ser demonstradas por meios virtuais. Além de terem mais recursos para pesquisas e métodos que influenciaram significativamente no aumento de seus conhecimentos, os quais serão de grande valia para seu desenvolvimento acadêmico, profissional e psicológico.

Embora muitas vantagens tenham sido apresentadas com a chegada de recursos tecnológicos, em especial, os que fazem parte da internet, não podemos deixar de destacar os males existentes, pois em toda criação teremos os pontos positivos e negativos.

As crianças e os adolescentes viraram alvos dos algozes, que se aproveitando desta fase, no primeiro momento de total inocência e depois achar que de tudo sabe e está preparado para a vida. E em ambas as fases, encontraremos malfeitores dispostos a se utilizar de tal vulnerabilidade para praticar suas condutas criminosas.

Concluímos que os cybercrimes atingem internautas do mundo inteiro, porém alguns países já dispõem de lei e políticas de prevenção. No Brasil, as leis que foram sancionadas são muito brandas, somadocom a falta de material humano especializado para aprofundar as investigações e localizar os criminosos. Além disso, temos uma carência de políticas de prevenção que, ao nosso ver, deveriam começar pelos pais e pelas escolas, com objetivo de reduzir a chance do alvo infanto-juvenil ser vítima de crimes,os quais poderão trazer efeitos negativos por toda sua vida.

REFERÊNCIAS

[1] BRASIL. Lei nº 8.609, de 13 de julho de 1990. Recuperado em 25 de abril de 2018, from http://www.planalto.gov.br/ccivil_03/leis/L8069.htm.

[2] BRETAN, Maria Emilia Accioli Nobre, *VIOLÊNCIA SEXUAL CONTRA CRIANÇAS E ADOLESCENTES MEDIADA PELA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: ELEMENTOS PARA PREVENÇÃO VITIMAL*. Recuperado em 25 de abril, 2019, from https://www.teses.usp.br/teses/disponiveis/2/2136/tde-22042013-111456/publico/TESE_COMPLETA_MARIA_EMILIA_A_N_BRETAN_FD_USP2012.pdf

[3] Conceito extraído da Classificação Internacional de Doenças (CID) da Organização Mundial de Saúde (OMS). Recuperado em 25 de abril, 2019, from http://cid10.bancodesaude.com.br/cid-10-f/f654/pedofilia.

[4] EISENSTEIN E, Estefenon S. *Computador: ponto social ou abuso virtual?*. Adolesc Saude. 2006;3(3):57-60. Recuperado em 09 de abril, 2019, from http://adolescenciaesaude.com/detalhe_artigo.asp?id=136.

[5] FEUSER, Bruna Ceccone; PAVEI, Fernando; NETO, Pedro Zilli; ZOMER, Ramirez; PAVEI, Rodrigo. *A VULNERABILIDADE DA CRIANÇA E DO ADOLESCENTE NAS REDES SOCIAIS: NECESSÁRIA CAUTELA PARA A SEGURANÇA DO PUBLICO INFANTO-JUVENIL*. Recuperado em 01 de maio, 2020, from http://periodicos.unibave.net/index.php/constituicaoejustica/article/view/115.

[6] FONSECA, Franciele Fagundes; SENA, Ramony Kris R.; SANTOS, Rocky Lane A. dos; ORLENE, Veloso Dias; COSTA, Simone de Melo. *As vulnerabilidades na infância e adolescência e as políticas públicas brasileiras de intervenção*. Recuperado em 30 de março, 2020, from https://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-05822013000200019.

[7] MACHADO, Thiago José Ximenes. *Cibercrime e o crime no mundo informático: A especial vulnerabilidade das crianças e dos adolescentes*. Recuperado em07 de agosto, 2018, from https://bdigital.ufp.pt/handle/10284/6089.

[8] MENDOZA, Miguel Ángel. *Os 10 principais riscos na Internet para crianças e adolescentes*. Recuperado em 03 de maio, 2020, from https://www.welivesecurity.com/br/2018/05/21/principais-riscos-na-internet-para-criancas-e-adolescentes/.

[9] MONTEIRO, Ana Francisca Cunha. *A INTERNET NA VIDA DAS CRIANÇAS: COMO LIDAR COM PERIGOS E OPORTUNIDADES*. Recuperado em 25 de junho, 2019, from encurtador.com.br/abqKT.

[10] PEREIRA, Marília do Nascimento. *A SUPEREXPOSIÇÃO DE CRIANÇAS E ADOLESCENTES NAS REDES SOCIAIS: necessária cautela no uso das novas tecnologias para a formação de identidade*. Recuperado em 10 de maio, 2020, from http://coral.ufsm.br/congressodireito/anais/2015/6-14.pdf.

[11] SANCHES, Rogério Cunha. *CODIGO PENAL para concursos. 9ª ed. Revista, ampliada e atualizada*. Editora: Jus Podivm, 2016.

[12] SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallas Tomaz. *RELAÇÕES JURÍDICAS VIRTUAIS: ANÁLISE DE CRIMES COMETIDOS POR MEIO DO USO DA INTERNET*. Recuperado em 25 de abril, 2019, from http://egov.ufsc.br/portal/sites/default/files/3952-21333-1-pb.pdf.

[13] SILVA, Rosane Leal da; VERONESE, Josiane Rose Petry. *Os crimes sexuais contra criança e adolescente no ambiente virtual*. Recuperado em 19 de abril, 2019, from http://www.ambito-juridico.com.br/site/index.php?artigo_id=6634&n_link=revista_artigos_leitura.

[14] SOUZA, Dercia Antunes de; OLIVEIRA, Joyce Alessandra de Moraes. *USO DE TECNOLOGIAS DIGITAIS POR CRIANÇAS E ADOLESCENTES: POTENCIAIS AMEAÇAS EM SEUS INTER-RELACIONAMENTOS*. Recuperado em 01 de maio, 2020, from https://www.aedb.br/seget/arquivos/artigos16/952473.pdf.

Versão em inglês da cartilha de prevenção para auxiliar adolescentes sobre os cibercrimes e cibersegurança

Question 1. **What is the Internet?**

Answer 1 –

Before we talk about the concept of the Internet, let's understand what a computer network is. When we link two or more devices together, making them talk to each other, we can call such a structure a network.

Now that we know what a network is, we can define the Internet as the interconnection of several computer networks spread around the world.

For better understanding we will illustrate with the following figure..

Representation of the Internet. Image extracted from *https://www.ufpb.br/ccae/contents/imagens/internet.jpg/image_view_fullscreen* site

The devices are connected to the Internet through ISPs, which, by law, must keep information related to their customers' access for a certain period of time, which can help the police locate and identify possible cybercriminals.

Question 2. **What is Cyberspace?**

Answer 2 –

It is the nomenclature given to the virtual environment that is used by the Internet so that the user may communicate with other people by means of devices such as the computer, smartphones, etc., and thus explore diverse means such as e-mail (electronic mail), sites, social networks, e-commerce (electronic commerce), e-business (electronic business), among others. It is important to remember that this space has an immeasurable dimension, making it a danger to users who intend to explore it without a basic knowledge of cybersecurity

Cyberspace representation. Image extracted from *https://www.alfaiatedaweb.com/blogue/item/37-ciberespaco-e-a-seguranca* site

The figure above shows how unlimited this virtual space is, so we can have the true dimension, even, of how difficult it is to locate a cybercriminal, because they can be anywhere on this planet, and we still have to take into account the large amount of techniques that help them to mask their addresses, making it even more difficult to find their real geographic location. And the conclusion is the high degree of impunity of cybercriminals, which increases the occurrence of this type of crime, since it is noticeable how difficult it is to find the true culprit for the act. Thus, we can conclude that prevention is still the best way to protect yourself from these cyber attacks.

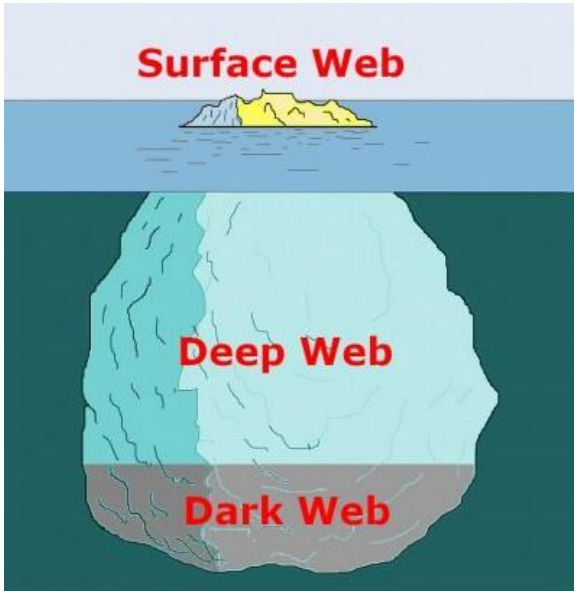
Question 3. **What is the Surface Web, Deep Web and Dark Net?**

Answer 3 –

The Surface Web is the part of the Internet where ordinary users access and benefit from the most diverse services such as email, websites (the most diverse), social networking, chats, and others.

Deep Web is the dark part of the Internet, where common users cannot enter. In this dark area, secret information flows between certain groups that want total privacy in their communications, and these groups can be set up by criminals or not.

The Dark Net is considered a part of the Deep Web, this is where criminals act practicing illicit acts such as child pornography, sale of weapons, drugs, organs, satanic sects, etc.



Representation of the Internet. Image extracted
https://tecnoblog.net/responde/como-acessar-deep-web-links/ site

These deeper layers of the Internet are accessed by specific programs, and obviously, to access certain communication networks, only people authorized by the servers that manage this link between computers. Thus, we can see the difficulty that the authorities face to be able to infiltrate and discover the crimes that circulate through this dark, or better, totally dark network. The deep web is only accessible through permissions and includes digital platforms and access to databases that can and are legal, most of the time, but, inaccessible to the generality of users.

Question 4. **What are Cybercrimes?**

Answer 4 –

These are crimes committed by means of devices that connect to the Internet:

Ex. 01: Hacking into a computer by means of programs, and thus, subtracting or damaging existing files.

Ex. 02: Using a social network to spread false accusations against someone.

Ex. 03: Making use of conversations in virtual rooms to arrange meetings and commit crimes such as robbery, extortion, kidnapping, etc.

Ex. 04: Using instant messaging applications, for example, WhatsApp to clone accounts, and commit fraud, pretending to be the owner of the account, and then requesting transfer of values or payment of bills.

Ex. 05: Forwarding the user to false sites, identical to the real ones, in order to obtain data such as passwords. And soon after, entering the accounts and practice the withdrawal of values or important data.

Ex. 06: Forwarding fakes e-mails requesting updates of data on bank accounts, or even government services, with the purpose of subtracting data such as IDs, passwords, logins, etc.

Illustration of a cybercriminal in action. Image extracted from *http://www5.tjba.jus.br/portal/cibercrimes-inscricoes-para-curso-sobre-o-tema-estao-abertas-ate-a-proxima-segunda-25/* site

Question 5. **What is Cybersecurity?**

Answer 5 –

Cybersecurity is about protecting devices, especially those that connect to the Internet, from malicious attacks, whether by means of programs or malicious people (hackers, crackers, etc.).

The programs that Internet users should have on their computers are antivirus and anti-malware programs, properly updated.

Cybersecurity illustration. Image extracted from *https://promovesolucoes.com/ciberseguranca-o-que-e/* site

It is important to know that cybersecurity is not simply limited to specific programs for protection, which must be installed on our computers and devices, but the behavior of users is what will actually decrease the chances of being a potential victim of cybercriminals.

It is important that the guardian always keeps the protection programs up to date to decrease the risks of the devices used by his or her child being infected by malware or viruses. However, constant vigilance is even more important, because attacks on teenagers usually happen on social networks and chat rooms, where cybercriminals use techniques to get close to them and seek to gain their victims' trust, and then put their criminal plan into practice, either by stealing important information or by arranging meetings to commit illicit acts.

Question 6. **What is Cyberbullying?**

Answer 6 –

Let's first deal with the concept of bullying. The term is of English origin and means repeated aggression and intimidation. The practice of such acts can be done through the Internet, either in a chat room, by email, social networks, among others.

These violent acts can cause physical injuries, however, we must warn that the most serious are the psychological consequences which can lead the adolescent to undergo psychiatric and psychological treatment, and many times even attempt his own life.

Illustrates a victim of Cyberbullying. Image extracted from *https://www.istockphoto.com/br/vetor/cyber-bullying-nas-redes-sociais-e-conceito-de-abuso-online-vector-flat-desenho-gm1213369038-352617628* site

At the age understood as adolescence (between 12 and 17 years old), the brain has not yet achieved the full formation of the communicating neurons, that is, the part of the brain that deals with reason cannot yet fully communicate with the part responsible for emotions. This is where the danger of a teenager being bombarded by provocation can be seen, considering that their emotions are exploding and they will not be able to deal with such acts in a rational way. Thus, the probability of psychological illness is extremely high, and the consequences are disastrous, affecting not only the victims but also their families and society, which somehow loses a member.

In these cases, seeking professional help, i.e., a psychologist can be essential to prevent irreparable damage from occurring, especially when there is a situation where the teenager has been a victim of cybercrime.

Question 7. **What is Cyberstalking?**

Answer 7 –

The English term stalking means stalking. So, cyberstalking is stalking through the Internet, that is, the victims are stalked and have their steps monitored. The use of photos of the victim to create false profiles can also occur, where the victim starts to receive pornographic content, unwanted advertisements, among others, making him/her psychologically ill due to this bombardment of unwanted information.

A typical figure to combat the conduct of stalking already exists in the penal code. This is provided in the article Art. 147-A, which reads: "Stalking someone, repeatedly and by any means, threatening his physical or psychological integrity, restricting his ability to move about, or in any way invading or disturbing his sphere of freedom or privacy. Penalty - confinement, from 6 (six) months to 2 (two) years, and fine. § 1 The penalty is increased by half if the crime is committed: I - against a child, adolescent or elderly individual; II - against a woman due to her condition as a female, under the terms of Paragraph 2a of art. 121 of this Code; III - by means of a competition of 2 (two) or more people, or with the use of a weapon. § The penalties in this article apply without prejudice to those corresponding to violence. § 3. Proceedings will only be carried out upon representation.

Illustration of Cyberstalking. Image extracted from *https://exame.com/pme/o-que-e-stalking-empresas/* site

We ratify that an adolescent's brain is not prepared to deal with mass criticism, because, as we have already commented, the part responsible for reason does not yet communicate well with the others, so he acts, exclusively, by feelings and emotions.

Question 8. **What is Fake News?**

Answer 8 –

The English expression means fake news and is widely used on the Internet to spread information that is not true, causing a large population mass to believe and spread such content. Often this fake news causes panic in society, and usually has an ideological, religious, political, etc. nature. This news often leads the population to commit thoughtless acts. This is why it is important to always check the source in order to avoid making mistakes.

Fake News Illustration. Image extracted from *https://www.agazeta.com.br/artigos/fake-news-no-passado-eram-chamadas-simplesmente-de-mentira-0620* site

We emphasize that these false stories can be directly related to the offense of slander, where a false scenario can be created and a person can be blamed for a crime that he or she did not commit, for example, spreading the word on social networks that a person committed the crime of rape of a child, when the accusation is false. In the same idea, we have the offense of defamation, where a false situation can be spread, which will directly affect the reputation of the victim in society, for example, saying that a certain person was in a house of prostitution, and thus ruining the marriage of this person.

It is very important to point out that once false information is propagated, it becomes very complicated to undo, because the speed and dimension it takes are often unimaginable. Information posted on the net propagates independently and is not erased by its repetition on the Internet/Web, running simultaneously with a possible correction, with both versions coexisting.

We advise that any and all content, before being published or reposted and, thus, propagated by the Internet user, should be checked for veracity, otherwise you may be feeding a Fake News.

Question 9. **What are Computer Viruses and Malware?**

Answer 9 –

A computer virus is nothing more than a little program that comes hidden inside games, documents, programs (various) etc. and has the objective of damaging and causing malfunctions in computers. It is important that the user has a program called antivirus, and that it is always up to date so that it can detect and eliminate any type of threat that can damage or corrupt the files on your computer.

The Malwares are malicious software that has the objective, in rules, to steal information and leave the computer vulnerable to be invaded by hackers. So, we can say that these softwares are installed on the computer, with bad intentions, without the owner's authorization.

Illustration of viruses and malware. Image extracted from *https://super.abril.com.br/mundo-estranho/como-funciona-um-virus-de-computador* site

The main and best known viruses, malware and malicious techniques are:

- **Trojan Horse** – A program that once installed on a computer, leaves it vulnerable to being invaded by cybercriminals. This software can come together with the installation of a game or any other application available for free on the Internet, and, after properly implanted in the computer, is intended to capture any information typed, from passwords to conversations in chat rooms or any application that has this purpose.
- **Ransomwares** – A program that puts passwords on personal files and charges a fee to unlock them. Here the user can have a considerable economic loss.

- **Spyware** – These are programs installed on the user's computer, without the user realizing it. This software can come together with the installation of a game or any other application freely available on the Internet, and, after duly implanted in the computer, has the purpose of capturing all and any information typed, from passwords to conversations in chat rooms or any application that has this purpose.
- **Keylogger** – A program whose purpose is to capture everything the user types, especially in fields where data and passwords are entered.
- **Screenlogger** – A program that takes screenshots from time to time, that is, it lets cybercriminals know what operations the user is performing.
- **Phishing** – It is a type of attack that uses the ingenuity of people who access the Internet, because it uses simple mechanisms, making the information be passed on by the victim, convincing them to fill out forms that apparently were requested by serious companies, such as banks or even government agencies.
- **Pharming** – Programs that direct the user to a fake website, but which is similar to the original site, causing the user to enter their sensitive data and passwords, and these are captured by cybercriminals.
- **Macro Viruses** – These are viruses that are usually hidden behind text editor buttons, such as Microsoft Word, and that once activated, contaminate the computer, leaving it vulnerable.
- **Social Engineering** – A technique that uses the power of persuasion to make the user send the data to the criminal, without realizing that he is a victim, for example: pretending to be a bank employee and saying that he needs the data and password to update the account. In truth, it is a matter of taking advantage of the characteristics of the human being, his curiosity, greed or any other aspect that motivates the person to take the intended action, and thus become captive of the cybercriminals, being manipulated to do so.
- **Shoulder Surfing** – These are actions of malicious people who watch the user while he enters personal data and passwords into their systems.
- **Backdoor** – Once a computer is infected with this type of malware, it can be hacked and manipulated by the criminal when the time is right - this is a form of delayed control that allows a computer that is thus considered a zombie to be taken over at a later date.

Question 10. **What programs can be used to protect against some cybercrimes?**

Answer 10 –

The computers must have anti-virus and anti-malware software installed. The Windows operating system provides a tool called Defender. However, there is a variety of software for this purpose, including free software that can be downloaded and installed. On the other hand, we have the large antivirus software companies that charge for these tools, but that provide excellent protection, but the big secret to staying safe is that these programs are constantly updated, because every day there is a new variation of virus and malware.

Question 11. **What behaviors can be adopted to avoid cybercrime?**

Answer 11 –

As we have already seen, there are many ways in which cybercrimes can be committed, so a great deal of care must be taken to reduce, as much as possible, the possibility of becoming a potential victim of cybercriminals.

The precautions and behaviors that users should take when accessing the Internet are:Nunca instalar programas desconhecidos ou de fontes não oficiais.

- Never install unknown programs or programs from unofficial sources.
- Never open files you do not know the origin of.
- Never access web sites with dubious content.
- Avoid making banking transactions without certainty of the site's security.
- Keep your operating system updated, because security errors are constantly being corrected.
- Use browsers that have security features.
- Never pay boletos sent by strangers. Always confirm the true recipient.
- Never send your data or passwords over the Internet (email, chat, etc.).
- Never send nude or sensual photos to anyone, even if they are known to you.
- Never maintain contact with strangers.

Question 12. **What are virtual communities?**

Answer 12 –

It is very common for people to be interested in the same subjects, have the same beliefs and ideologies, practice the same activities, etc. So they create virtual media to exchange information on these topics, and for this they use websites, blogs, social networks and others, forming virtual communities. The big danger is that not always in these communities people are actually interested in these topics, but they use these resources to get close to people and commit some kind of illicit act.

Illustration of virtual communities. Image extracted from *https://comunidadesvirtuaisdeaprendizagem.wordpress.com/2014/10/12/importancia-das-comunidades-virtuais-de-aprendizagem-para-a-ead/* site

Question 13. **What are social networks? What are their objectives?**

Answer 13 –

Social networks are websites or applications that connect people through the Internet, and make them communicate and share photos, videos, texts, etc.

There are several objectives that we can highlight, among them:

- Make new friends.
- Keep in touch with friends around the world.
- Search for love relationships.
- Locate people.
- Know the tastes, ideologies, hobbies etc. of the people you are interested in.
- Search for jobs.
- Search for academic knowledge.
- Offer services and products.
- Protest against something or someone.
- Publicize books, articles, projects, social actions, etc.
- Campaigning for politics, solidarity, education, etc.
- Disseminate work.
- Increase visibility of the work activity developed.
- Search for business partnerships.

Social network illustration. Image extracted from *https://cakeerp.com/blog/redes-sociais/* site

Question 14. **What age range does the law consider an adolescent to be?**

Answer 14 –

According to the Child and Adolescent Statute, the age range to be considered an adolescent is from 12 years old to 17 years old. **ATTENTION**: check the law of your country.

Illustration of the Children and Adolescents Law. Image extracted from *https://www.novacandelaria.rs.gov.br/site/noticias/administracao/15967-13-de-julho---dia-do-eca-%E2%80%93-estatuto-da-crianca-e-do-adolescente* site

Question 15. **What is a vulnerable person? Why teens are considered vulnerable to cybercrime?**

Answer 15 –

Vulnerable people are those who are more likely to be victims of certain actions, such as robberies, thefts, fraud, rape, and others. When it comes to cybercrime, we can say that teenagers have a certain vulnerability, due to the fact that they are going through a phase of discovery, where self-affirmation and the desire to make decisions are considerably relevant, and there is also the issue of not fearing the consequences they may have if they use Internet access in an unrestrained manner.

We can also emphasize that consumerism in this phase is very high, and the desire to own certain objects, clothes, etc. may be a factor that facilitates the cybercriminal to approach

his victim, and this contact occurs most often through social networks, where teenagers show their tastes and desires.

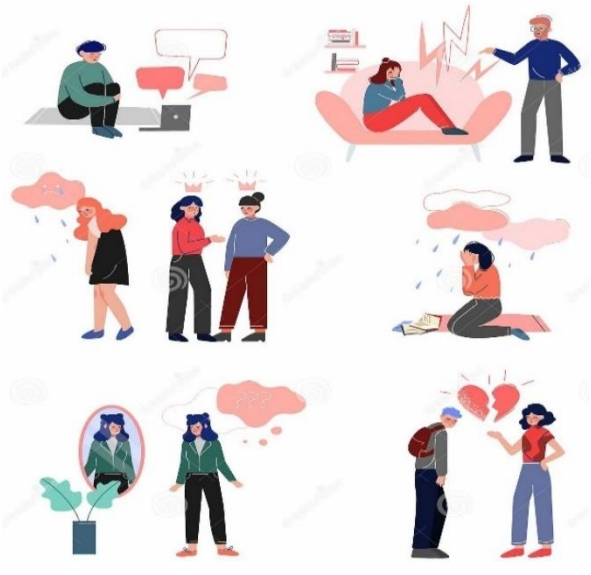


Illustration of adolescent vulnerability. Image extracted from *https://pt.dreamstime.com/adolescentes-deprimidos-lan%C3%A7am-conflito-ciberbuloso-com-depress%C3%A3o-dos-pais-amor-sem-resposta-problemas-de-puberdade-adolescente-image194711688*site

We have two important parts of the brain, among many others, the part that deals with feelings and the part that deals with reason. Adolescents have not yet formed 100% of this part responsible for reason, which is why they cannot have a logical view of a certain attitude, and this is a prime factor for them to be targeted by cybercriminals.

Question 16. **Why the teenager is easily manipulated, psychologically?**

Answer 16 –

Adolescents do not yet have their communication neurons fully ready, that is, the transmitters that make the information pass through the field of reason, inside the brain, have not yet been formed. Thus, the brain is driven by emotion.

Remember that adolescents seek self-affirmation, so that they can be accepted by their peers. For this reason, they can be tricked and manipulated by a cybercriminal who has this knowledge. This is because the cybercriminal will reach the weak point of the victim's psyche,

making the victim think that he or she is acting correctly and in accordance with the standards of the communities to which they belong.

Manipulation illustration. Image extracted from *https://pensarbemviverbem.com.br/6-tipos-sutis-de-manipulacao-psicologica/* site

This manipulation can lead the teenager to commit illicit behavior, as well as actions that will drastically affect his or her psychological state, and can make him or her dependent on psychotropic medication, or even lead him or her to commit suicide.

Question 17. **What strategies are used to attract teenagers?**

Answer 17 –

The technique used to attract teenagers, making them potential victims, is by showing similar behavior and tastes, that is, by participating in groups that arouse interest, whether they are about music, political ideologies, clothing styles, aesthetics, among other issues that guide this phase of transformation that is adolescence.

After the cybercriminals have the first contact with their possible victims, they try to get to know their victims' behavior even better and tend to make them think that they have found a friend or a perfect match, who think exactly the same way and have the same tastes. Consequently, they start to trust and become manipulated, which can lead to a series of problems, including psychological ones.

Illustration of how teenagers are attracted. Image extracted from *https://www.showmetech.com.br/quais-sao-as-tendencias-entre-os-jovens-da-geracao-z-em-2019-segundo-pesquisa/* site

Adolescence is a phase marked by dreams of consumption, which is a feature exploited by cybercriminals, since they offer products that young people are interested in owning. Thus, adolescents are easily attracted and are soon being totally manipulated by these criminals. We emphasize that the virtual means can only be a tool for the practice of face-to-face crimes, that is, the criminal uses the resources of technology to get closer to the victim and practice the most diverse criminal modalities.

Question 18. **What the Statute of the Child and Adolescent has to say about crimes committed over the Internet?**

Answer 18 –

In a very direct and simple way, we will present the offenses brought by the E.C.A. (Statute of the Child and Adolescent), which are directly related to the Internet, and which must be recognized by those responsible if one of these actions that we will mention below occurs. **ATTENTION**: check the law of your country.

Offense 1 - Producing, reproducing, directing, photographing, filming or recording, by any means, scenes of explicit sex or pornography involving children or teenagers.

Offense 2 - Selling or exposing for sale photographs, videos or other records containing explicit sex or pornographic scenes involving children or adolescents.

Offense 3 - Offering, exchanging, making available, transmitting, distributing, publishing or divulging by any means, including through computer or telematics systems, photographs, videos or other records containing explicit sex or pornographic scenes involving children or adolescents.

Offense 4 - Acquiring, possessing or storing, by any means, a photograph, video or other form of recording that contains a scene of explicit sex or pornography involving a child or adolescent.

Offense 5 - Simulating the participation of a child or adolescent in a scene of explicit sex or pornography by means of adulteration, editing or modification of a photograph, video or any other form of visual representation.

Offense 6 - Enticing, harassing, instigating or forcing, by any means of communication, a child to commit libidinous acts.

Do you know what the term "explicit sex scene or pornography" means?

For the purposes of the crimes foreseen in this Law, the expression "explicit sex scene or pornography" includes any situation that involves a child or teenager in explicit sexual activities, real or simulated, or exhibition of the genital organs of a child or teenager for primarily sexual purposes.

IMPORTANT

There are several crimes that are committed against teenagers in the penal code and that can be applied if committed through the Internet, for example, threat, illegal constraint, defamation, insult, persecution, among others.

Illustration of a victim of cybercrime. Image extracted from *https://www.centrosermais.com/cyberbullying-o-que-precisa-saber/* site

Question 19. **Teenagers can commit criminal acts over the Internet?**

Answer 19 –

The Statute of the Child and Adolescent establishes that adolescents do not practice a crime but an infraction, since the punishments are different from those applied to adults. We emphasize, however, that there are penalties that can bring as a consequence, the deprivation of liberty for application of socio-educational measures. **ATTENTION**: check the law of your country.

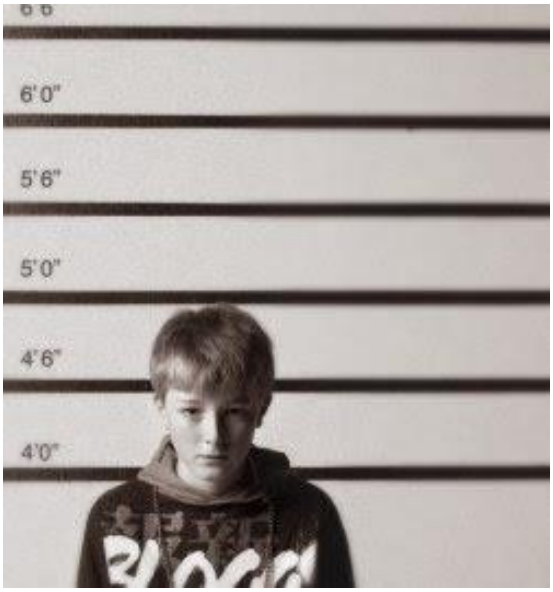


Illustration of an adolescent being punished for an infraction. Image extracted from *https://veja.abril.com.br/coluna/cacador-de-mitos/mito-os-adolescentes-cometem-menos-de-1-dos-homicidios-do-brasil-e-sao-36-das-vitimas/* site

Question 20. **What would be the ideal access time for a teenager??**

Answer 20 –

We do not have an ideal time for Internet access, because we must analyze some factors, such as:

- Research time (between 1 and 2 hours)
- Entertainment time (between 1 and 2 hours)
- Time for work (on average 8 hours - with short rest intervals - which would make a total of 6 hours and 30 minutes in front of the computer screen)

We can state that for every 50 minutes in front of the screen, we should stop for at least 10 minutes, which we can use to have small meals, drink water, wash our faces, do our physiological needs, in short, take our minds off that focus.

Illustration of excessive Internet access time. Image extracted from *https://paranoiasnfm.wordpress.com/2012/01/14/vicio-internet-alcool-drogas/* site

Question 21. **What harm can excessive hours connected to the Internet bring?**

Answer 21 –

There are many harms that unbridled access can bring, both to physical and psychological health. We can cite some of these evils.

- Problems with vision, since the intense light beams that come in without a break and for long periods every day can cause damage to the eyeball.
- Diet can be compromised, since teenagers spend hours and hours concentrating and staring at the computer screen or smartphone, and forget to eat. Such attitudes can be harmful to various organs, especially the stomach.
- Problems in the nerves of the hand, which can bring consequences such as RSI (Repetitive Strain Injury), which is considered a syndrome consisting of a group of diseases - tendinitis, tenosynovitis, bursitis, epicondylitis, carpal tunnel syndrome,

trigger finger, thoracic outlet syndrome, round pronator syndrome, myalgias -, which affects muscles, nerves, and tendons of the upper limbs mainly, and overloads the musculoskeletal system. This disorder causes pain and inflammation and can alter the functional capacity of the affected area.

- The strong incidence of light from the computer screen can cause insomnia, since the brain is activated when it should be resting.
- Pain in the shoulders, neck and spine, due to the user staying in the same position for hours.
- Memory loss can occur, especially in cases of users who are addicted to games, because they tend to concentrate too much and end up not feeding the brain with other information.
- The google effect affects the human brain in such a way that it starts to store the least amount of information, since it is conditioned to search everything easily in this search tool - also affecting the memory and the ability to memorize, and consequently, understanding and learning;
- The nomophobia is the fear of not having technology present at all times, that is, the user becomes totally dependent on devices that connect to the Internet, as an example, we have the use of smartphones, which have become an inseparable tool of people.
- Phantom ringing syndrome where the brain is so connected to the cell phone that the user feels vibrations and hears ring tones without the phone emitting such signals. This can lead to compulsive behavior and anxiety attacks.
- And lastly, FOMO (fear of missing out) is the fear of missing something, that is, the need to know what other people are doing, thus generating anxiety crises

Illustration of the health problems that can be caused by excessive hours on the Internet. Image extracted from the *https://www.tecmundo.com.br/internet/6449-jovens-podem-ter-problemas-de-saude-se-expostos-a-mais-de-tres-horas-na-internet.htm* site

Question 22. **What are Internet Challenges and what are their goals?**

Answer 22 –

Many are the challenges that arise and spread over the Internet, i.e. dangerous practices that endanger the health or life of the participants or others. Examples are:

Blue Whale - This challenge has the objective of making the participant perform acts that would diminish their fear of death, and ultimately, induce suicide.

Devil's Alphabet - Makes teenagers mutilate themselves by using sharp objects to draw Chinese letters on their hands, on pain of being cursed.

Deodorant Challenge - Participants must inhale the aerosolized substance and keep their mouths closed for as long as possible. This challenge can lead to cardiac arrest, due to the substances that make up these products.

Cold water challenge - The goal is to pour a bucket of ice over the head, which carries a risk of hypothermia.

Salt and ice - Makes the participants put salt and ice on their hands and keep them closed for as long as possible. As a consequence, the participant can have severe burns.

Fire game - The participant pours flammable product on their body and lights it, lights the fire, and runs off to throw themselves into a pool, lake, etc. The risk here is notorious, a serious burn can occur.

Game of Momo - A doll manipulated by the criminal, who makes videos to children and teenagers, asking them to do some macabre challenges that can lead to death.

Illustration of the challenges of the Internet. Image extracted from *https://www.curiosidades.com.br/2019/04/desafios-mais-perigosos-da-internet/* site

Question 23. **What evils can social networks bring?**

Answer 23 –

Teenagers generally use social networks to communicate with their peers, and this way of interacting requires demonstrations of attitudes that are admired by them.

Posting pictures in certain places, with certain clothes, with certain influential people, all these are posted, and the teenager anxiously waits for the likes. The problem is when the criticism, cyber-bullying, and other attitudes come, which mess with their psychology, causing them to have anxiety attacks, panic syndrome, or depression, which can have drastic consequences, such as suicide.

Teenagers are not prepared to receive any kind of mass criticism, and social networks are a specialist in this type of action. Once a photo or publication is posted on the social network, in a matter of minutes it becomes news to the whole world, and consequently comes a bombardment of comments, which are often unpleasant and deeply affect those who are in the process of maturing and do not know how to deal with certain situations that life imposes on us - even for adults, these situations can be extreme, let alone for teenagers.

Illustration of the evils of social networks. Image extracted from *https://www.vittude.com/blog/impactos-redes-sociais-saude-mental/* site

We emphasize that, the exposure made in social networks can facilitate the commission of crimes, since they show people's routines, such as the school they study, the restaurant they go to, the goods they own, where they live, their financial conditions, their friendships, that is, it literally exposes all the information necessary for a criminal to plan an attack.

Question 24. **What are nudes? What is sextorsion?**

Answer 24 –

The term comes from the English language and means naked. Today it is very common for young people to take pictures that show intimate parts of their bodies and then send them to people in their relationships or even to strangers, trusting that they will not spread the images. This is where sextortion comes in, which is extortion, that is, the criminal demands money from the victim in order not to spread the intimate pictures over the Internet. The consequence of this is that many teenagers commit suicide because of the shame they feel for such behavior and for not being able to handle the thousands of insults they are subjected to. Sometimes, instead of money, blackmail is used to get the cybercriminal to force the teenager to perform certain types of actions, including sexual acts, in exchange for not releasing the images.

Sextorsion illustration. Image extracted from *https://prezi.com/p/rrpzqm_40iio/grooming-sexting-sextorsion/* site

We emphasize that you should never send sensual or sexual photos or videos, even to people you believe to be trustworthy. Because, even if these people do not send the images, the device may be lost, and the stored content may be accessed by a stranger, and here we may have two paths: use this private content to extort the owner, or publish it on the Internet for the simple pleasure of it, which, either way, will bring irreparable damage.

Question 25. **What are the main offenses that can go from virtual to real life?**

Answer 25 –

Many cybercriminals use the Internet only as a tool to commit crimes in the real world. The most common crimes are:

- **Robbery:** After knowing the victim's financial conditions, he arranges friendly meetings to then steal the victim's belongings, using violence or serious threat.
- **Larceny:** Knowing the victim's routine, the criminal may plan to enter the victim's home and take away the victim's belongings.
- **Robbery followed by death:** With the objective of obtaining valuables or goods of considerable value, the criminal, who has knowledge of the victim's wealth, plans the attack by taking the victim's life to achieve his or her goal.
- **Stupping:** He arranges meetings with the victim and makes her believe his fanciful stories, inducing her to give him valuables or belongings.
- **Rape:** The rapist usually chooses certain profiles of people to carry out his attacks, and these can easily be found on social networks, for example, after getting close and gaining the victim's and even the family's trust, he commits the crime of rape.
- **Rape of the vulnerable:** With the same techniques used to commit rape, the criminals also rape minors under the age of 14, who are considered vulnerable by the Brazilian penal code.
- **Extortion through kidnapping:** By knowing the victim's possessions, as well as his or her routine, the criminal plans the kidnapping with the objective of obtaining values as a ransom.
- **Murder:** The criminal who intends to kill the victim pretends to be a third party, arranges a friendly meeting, and then attracts the victim in order to take his or her life.

Illustration of crimes initiated on the Internet and consummated in the real world. Image extracted from *https://masterjuris.com.br/principais-crimes-contra-o-patrimonio/* site

Question 26. **How cybercriminals operate?**

Answer 26 –

There are several types of cybercriminals, and their modus operandi and goals will be quite specific. We will show you the nomenclatures given to cybercriminals and what they usually attack and how they act.

- **Cybercriminal:** People who use the Internet to commit the most diverse types of crimes, such as: fraud, extortion, theft, defamation etc.
- **Lammer:** People who do not possess any knowledge, such as a hacker, but who use ready-made tools to carry out their attacks.
- **Hackers:** These are people with advanced knowledge who test this knowledge to modify software and hardware.
- **Crackers:** They are invaders, in other words, real criminals, who use their knowledge to harm a system or people.
- **Phreaker:** A specialist in breaking into telephone systems.
- **Carder:** A specialist in credit card fraud.
- **War Driver -** Is a specialist in wireless networks, that is, he takes advantage of their vulnerability to break into them.
- **Defacers:** These are people who break into sites and modify the layout, leaving their trademark, like a kind of graffiti, with the objective of showing off their feat to other cybercriminals.
- **Script Kiddies:** These are inexperienced people who look for easy targets to apply their little knowledge and thus obtain some profit.
- **Guru:** These are people with a very high level of knowledge; we can say that they are the father of hackers.

Illustration showing the difference between Hackers and Crackers.
Image extracted from *https://brainly.com.br/tarefa/12242173* site

Question 27. **What is Virtual Surveillance Capitalism?**

Answer 27 –

The term surveillance capitalism was created to emphasize that data nowadays has a very significant economic value and can be sold and money can be made out of it. The Internet monitors and compiles all users' data in order to find out their interests and thus boost the consumer goods industry.

It is no wonder that when the user searches for a certain product, this begins to appear, in the form of advertising, in email, ads within other sites, and even phone calls offering the searched product. All this is not by chance, we can affirm that everything that is done through the Internet is captured and processed, and that this information is valuable for many interested parties.

Illustration of surveillance capitalism. Image extracted from *https://www.newslinereport.com/negocios/nota/capitalismo-de-la-vigilancia-la-regulacion-a-monopolios-tecnologicos-* site

Question 28. **What psychological consequences victims of cybercrime may experience?**

Answer 28 –

It is of great importance to address the psychological aspect that can be strongly affected in adolescents who become victims of cybercrime. It is worth noting that if, the psychological aspect is affected, it is very likely that some organ of our body will manifest itself negatively, i.e., turning into a physical illness.

Some psychological illnesses can seriously affect a cybercrime victim, among them:

- **Anxiety -** This is a disease that affects the psychological to the point that it causes the mind to have excessive or constant worries that something negative is going to happen. These anxiety attacks can also bring on physical illnesses. E.g.: Someone who anxiously waits for people to comment on his posts on social networks.
- **Depression -** This is a psychological disorder that causes the affected person to become sad and no longer feel like doing tasks that were previously pleasurable. E.g., being deluded by the posts made by people on the Internet, which can cause a feeling that everyone is happy and successful but you.
- **Panic Syndrome -** These are sudden and intense anxiety attacks with strong feelings of fear and uneasiness, accompanied by physical symptoms. E.g.: Fake News showing false statistics about illnesses, which makes you feel frightened that you will be stricken with illness and die.
- **Accelerated Thinking Syndrome -** This is a symptom associated with anxiety which, due to the large amount of information processed daily, causes the mind to become agitated, hyper-thinking, impatient, etc., and can lead to depression, panic syndrome, stress, etc. E.g.: People who spend their days being bombarded by information coming from e-mails, WhatsApp, Instagram, Facebook, websites, etc.
- **Nomophobia:** It is the irrational fear of losing your cell phone or being unable to use the phone for some reason, such as the absence of a signal, or being victim of a virus which made the phone stop working, or the termination of the data package or the battery running out. E.g.: People who have become dependent on their cell phones because all their information and activities are carried out through them.

Question 29. **Qual delegacia de polícia especializada procurar em caso de cibercrimes?**

Answer 29 –

Within the structure of civil police stations, we have a specialized one called the Division of Prevention and Repression of Technological Crimes (DPRCT). Its purpose is to identify and locate cybercriminals. It can then deliver information to the judiciary so that they can be punished according to the criminal legislation in force in the country. **ATTENTION**: check the law of your country.

Question 30. **What social problems can be caused by not reporting cybercrimes?**

Answer 30 –

When a victim or his or her legal representative fails to report the offense to the competent police authorities, the phenomenon called the Dark Cipher is strengthened, which consists in the authorities not knowing about the crimes committed. We also emphasize that such conduct can feed the practice of cybercrime, since cybercriminals go unpunished, thus victimizing more and more members of society.

Autorização da comissão de ética da plataforma Brasil para realização da pesquisa

FIBRA CENTRO UNIVERSITÁRIO — FACULDADE INTEGRADA BRASIL DA AMAZÔNIA - FIBRA — Plataforma Brasil

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: A CIBERSEGURANÇA PARA ADOLESCENTES
Uma proposta para a sua comunicação

Pesquisador: THIAGO XIMENES

Área Temática:

Versão: 2

CAAE: 55040221.0.0000.8187

Instituição Proponente: Universidade Fernando Pessoa/Fundação Ensino e Cultura Fernando Pessoa

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.310.137

Apresentação do Projeto:

A pesquisa tem como objetivo principal, desenvolver uma proposta de modelo a qual possa auxiliar todos os envolvidos nas questões perigosas de cibersegurança relacionada ao contexto específico que diz respeito ao acesso descontrolado e desvigiado de tal público, aumentando consideravelmente os riscos de se tornarem vítimas de ações criminosas.

Objetivo da Pesquisa:

Explicitar e desenvolver um modelo de despiste que identifique o potencial de um adolescente tomar comportamentos de risco no contexto de
digital;

Definir e aprofundar os conceitos de cibercrime, cibersegurança, ameaças ciber e comportamentos de risco em adolescentes;

Organizar as dimensões de um modelo de comportamento de risco associado com as práticas digitais de

Endereço: Av Gentil Bittencourt nº 1144 - 4º andar
Bairro: NAZARE **CEP:** 66.040-174
UF: PA **Município:** BELEM
Telefone: (91)3266-3110 **E-mail:** eticacomite@fibrapara.edu.br

FACULDADE INTEGRADA BRASIL DA AMAZÔNIA - FIBRA

Continuação do Parecer: 5.310.137

adolescentes

Propor um modelo de comunicação para prevenção e cibersegurança para adolescentes

Avaliação dos Riscos e Benefícios:

Os riscos e benefícios foram apresentados e estão de acordo com a proposta da pesquisa e com os princípios éticos

Comentários e Considerações sobre a Pesquisa:

Uma pesquisa de relevância comprovada, pois, contemporaneamente, enfrentamos diariamente situações de insegurança na utilização das novas tecnologias associadas à internet.

Considerações sobre os Termos de apresentação obrigatória:

O TCLE foi apresentado.

Recomendações:

Sem recomendações.

Conclusões ou Pendências e Lista de Inadequações:

Não há pendências nem inadequações.

Considerações Finais a critério do CEP:

APROVADO

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1836061.pdf	10/03/2022 11:24:45		Aceito
Projeto Detalhado / Brochura Investigador	Projeto_Plataforma_Brasil_atualizado.pdf	10/03/2022 11:23:42	THIAGO XIMENES	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	TCLE.pdf	17/11/2021 19:03:50	THIAGO XIMENES	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	Declaracao_Orientador_Plataforma_Brasil_ximenes.pdf	19/10/2021 09:18:06	THIAGO XIMENES	Aceito
Projeto Detalhado	Projeto_Plataforma_Brasil.pdf	19/10/2021	THIAGO XIMENES	Aceito

Endereço: Av Gentil Bittencourt nº 1144 - 4º andar
Bairro: NAZARE **CEP:** 66.040-174
UF: PA **Município:** BELEM
Telefone: (91)3266-3110 **E-mail:** eticacomite@fibrapara.edu.br

FACULDADE INTEGRADA BRASIL DA AMAZÔNIA - FIBRA

Continuação do Parecer: 5.310.137

/ Brochura Investigador	Projeto_Plataforma_Brasil.pdf	09:17:15	THIAGO XIMENES	Aceito
Folha de Rosto	folha_de_rosto_carimbada.pdf	19/10/2021 09:10:54	THIAGO XIMENES	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

BELEM, 24 de Março de 2022

Assinado por:
CINTHIA BRIGIDA BRITO DE MORAES
(Coordenador(a))

Endereço: Av Gentil Bittencourt nº 1144 - 4º andar
Bairro: NAZARE **CEP:** 66.040-174
UF: PA **Município:** BELEM
Telefone: (91)3266-3110 **E-mail:** eticacomite@fibrapara.edu.br