UNIVERSIDADE DO ESTADO DA BAHIA – UNEB
Gestão e Tecnologias Aplicadas à Educação – GESTEC

Programa de Pós-Graduação *Stricto-Sensu*
Mestrado Profissional Gestão e Tecnologias Aplicadas à Educação
Área de Concentração 2: Processos Tecnológicos e Redes Sociais

DIREITOS HUMANOS DIGITAIS:
Educação e segurança digital como ferramentas para o enfrentamento do Cyberbullying.

ELBA LÚCIA DE CARVALHO VIEIRA

SALVADOR - BAHIA
2019

DIREITOS HUMANOS DIGITAIS:
Educação e segurança digital como ferramentas para o enfrentamento do Cyberbullying

Dissertação apresentada ao Programa de Pós Graduação em Gestão e Tecnologias Aplicadas à Educação - GESTEC, da Universidade do Estado da Bahia – UNEB, como requisito para obtenção do título de Mestre.
Orientador: Prof. Dr. José Cláudio Rocha

SALVADOR - BAHIA
2019

ELBA LÚCIA DE CARVALHO VIEIRA

FICHA CATALOGRÁFICA

Sistema de Bibliotecas da UNEB
Dados fornecidos pelo autor

DE CARVALHO VIEIRA , ELBA LÚCIA

DIREITOS HUMANOS DIGITAIS: Educação e Segurança Digital como ferramentas para o enfrentamento do Cyberbullying / ELBA LÚCIA DE CARVALHO VIEIRA .-- Salvador, 2018.
108 fls : il.

Orientador(a): JOSÉ CLÁUDIO ROCHA .
Inclui Referências
Dissertação (Mestrado Profissional) - Universidade do Estado da Bahia. Departamento de Educação. Programa de Pós-Graduação em Gestão e Tecnologias Aplicadas à Educação - GESTEC, Câmpus I. 2018.

1.Direitos Humanos Digitais. 2.Cyberbullying. 3.Segurança Digital.

CDD: 001

FOLHA DE APROVAÇÃO

"DIREITOS HUMANOS DIGITAIS: A EDUCAÇÃO E SEGURANÇA DIGITAL COMO FERRAMENTAS PARA O ENFRENTAMENTO DO CYBERBULLYING E CRIMES DIGITAIS"

ELBA LÚCIA DE CARVALHO VIEIRA

Trabalho de Conclusão de Curso apresentado ao Programa de Pós-Graduação *(Scricto Sensu)* Gestão e Tecnologias Aplicadas à Educação, Área de Concentração I – Gestão da Educação e Redes Sociais, em 30 de agosto de 2018, como requisito parcial para obtenção do grau de Mestre em Gestão e Tecnologias Aplicadas à Educação, pela Universidade do Estado da Bahia, composta pela Banca Examinadora:

Prof. Dr. José Cláudio Rocha
Universidade do Estado da Bahia - UNEB
Doutorado em Educação
Universidade Federal da Bahia – UFBA

Prof. Dr. Felipe Rodrigues Bomfim
Universidade do Estado da Bahia - UNEB
Doutorado em Difusão do Conhecimento
Universidade Federal da Bahia – UFBA

Prof. Dr. João Dias de Queiroz
Universidade Federal da Bahia – UFBA
Doutorado em Difusão do Conhecimento
Universidade Federal da Bahia – UFBA

AGRADECIMENTOS

A Deus.

Ao meu pai (*in memorian*) e minha mãe. Formadores da minha base e suporte da minha educação.

Ao meu irmão de sangue e minha irmã de vida.

Às crianças da minha vida.

À minha família e meus amigos.

A todos os meus professores e orientadores.

A esta grande jornada chamada “VIDA”!

“Eu”

Você não me conhece.

Não digo o que sou, mas digo o que penso.

E penso que você não me conhece.

Se sua chance de pensar em mim
é mais forte do que o que sou,
o que digo,
o que vivo,
então, penso que você não me conhece.

Se estar comigo é achar em mim algo que não tenho,
então, sinto que você não me conhece.

Se seu coração é tão rebelde quanto o meu,
a sua mente tão modesta quanto a minha,
e a sua alma é tão sedenta de humanidade,

Então, sei que você me achou.

Elba Vieira.
(“A Gaveta do Meio” – Ed. Scortecci)

RESUMO

Direitos Humanos Digitais: educação e segurança digital como ferramentas para o enfrentamento do Cyberbullying.

As grandes mudanças tecnológicas, percebidas nas últimas décadas, transformaram o mundo numa sociedade digital, onde indivíduos, comunidades, sociedades, governos, organizações e países utilizam, massivamente, tecnologias de informação e comunicação (TICs) para diversos fins. A humanidade tem se beneficiado destas TICs e, em especial, da Internet que é uma rede de alcance mundial que utiliza um diversidade de tecnologias para sua existência. Por outro lado, caos, ameaças e crimes também rondam os ambientes digitais. Um deles é o "Cyberbullying", também conhecido como bullying digital, quando pessoas sofrem ameaças e ações abusivas através do uso de tecnologias. Neste sentido, considerando que o mundo digital "espelha" o mundo físico (os indivíduos são os mesmos), os direitos humanos fundamentais dos indivíduos devem ser igualmente honrados e preservados para todos, em qualquer lugar, incluindo na vida digital, o qual pode ser tratado como "Direitos Humanos Digitais".

A pesquisadora, como profissional experiente das áreas de tecnologia e segurança digital, acompanhou o avanço dos riscos cibernéticos, ao longo de sua trajetória pela atuação em várias Organizações, aplicando atividades de sensibilização em segurança digital, onde observou resultados positivos e culminaram na redução de incidentes de segurança nas Organizações em que atuou, percebendo a importância de sensibilizar pessoas. Esta percepção transformou-se em inquietações pessoais que se transformaram na iniciativa de fazer pesquisa na área de educação, visando a investigação de temas que abordam os Direitos Humanos e, em especial, o Cyberbullying ou Bullying Digital. Passou a ser um objetivo da pesquisadora a construção de conteúdos em segurança digital que tivesse alcance social com acesso ao público. Assim nasceu a ideia da construção da cartilha educativa "Orientações para uma Internet mais humana" como forma de contribuir com orientações de segurança para comunidades, escolas, famílias, profissionais de diversas áreas e, principalmente, os jovens, indivíduos ainda em formação e grandes vítimas do Bullying, digital ou não.

Neste contexto, esta pesquisa objetiva fazer uma abordagem sobre os Direitos Humanos no mundo digital da Internet e a importância na aplicação de ações educativas em segurança digital que sirvam de alerta para usuários da Internet e enfrentamento contra práticas abusivas como o "CyberBullying". O direito à privacidade, à proteção dos dados pessoais, contra o racismo, contra a pornografia infantil, contra a homofobia, também são assuntos abordados na pesquisa. É uma pesquisa aplicada, por ter como objetivo gerar conhecimentos para possível solução de problemas específicos e é também exploratória, investigando o tema sob diversos ângulos e aspectos.

Palavras-chave: Direitos Humanos Digitais. Cyberbullying. Segurança Digital.

ABSTRACT

Digital Human Rights: Education and digital security as tools for coping with Cyberbullying.

The great technological changes, perceived in the last decades, have transformed the world into a digital society, where individuals, communities, societies, governments, organizations and countries massively use information and communication technologies (ICTs) for various purposes. Humanity has benefited from these ICTs, and especially from the Internet, which is a worldwide network that uses a diversity of technologies for its existence. On the other hand, chaos, threats and crimes also surround digital environments. One of them is "Cyberbullying", also known as digital bullying, when people suffer threats and abusive actions through the use of technologies. In this sense, considering that the digital world "mirrors" the physical world (individuals are the same), the fundamental human rights of individuals must be equally honored and preserved for everyone, everywhere, including digital life, which can be treated as "Digital Human Rights".
The researcher, as an experienced professional in the areas of technology and digital security, followed the advance of cybernetic risks, throughout her career by acting in various organizations, applying awareness activities in digital security, where she observed positive results and culminated in the reduction of incidents security in the Organizations in which it acted, realizing the importance of sensitizing people. This perception has become personal concerns that have become the initiative of doing research in the area of education, aiming the investigation of topics that address Human Rights, and especially Cyberbullying or Digital Bullying. It became a goal of the researcher to build content in digital security that had social reach with access to the public. Thus, the idea of constructing the educational guide "Guidelines for a more humane Internet" was born as a way to contribute with safety guidelines for communities, schools, families, professionals from different areas and especially young people, individuals still in formation and great victims of bullying, digital or not. In this context, this research aims to make an approach on Human Rights in the digital world of the Internet and the importance in the application of educational actions in digital security that serve as a warning for Internet users and coping with abusive practices such as CyberBullying. The right to privacy, the protection of personal data, against racism, against child pornography, against homophobia are also issues addressed in the survey. It is an applied research, because it aims to generate knowledge for the possible solution of specific problems and is also exploratory, investigating the theme from various angles and aspects.

Keywords: Digital Human Rights. Cyberbullying. Digital Security.

LISTA DE FIGURAS

LISTA DE ABREVIAÇÕES

GESTEC – Gestão e Tecnologias Aplicadas à Educação.

TIC – Tecnologia da Informação e Comunicação.

UIT – União Internacional de Telecomunicações. Agência do Sistema das Nações Unidas dedicada a temas relacionados às Tecnologias da Informação e Comunicação.

UNEB – Universidade Estadual da Bahia.

SUMÁRIO

APRESENTAÇÃO: RESUMO DE UMA TRAJETÓRIA RUMO AO OBJETO DE PESQUISA

Perfil da Pesquisadora

A pesquisadora é uma profissional com larga experiência de 30 (trinta) anos atuando nas áreas de Tecnologia da Informação, Segurança da Informação, Riscos de Segurança e áreas correlatas, tendo participado de diversos projetos em Instituições (públicas e privadas) Financeiras, Governamentais e de Saúde, no Brasil (Bahia e São Paulo) e em Portugal (para projetos pontuais).

É mestranda em "Gestão e Tecnologias Aplicadas à Educação" (UNEB/GESTEC) e Pesquisadora do Centro de Referência em Desenvolvimento e Humanidades (CRDH/UNEB). Possui MBA em Administração (UNIFACS), especialização em Informática (UFBA) e graduação em Processamento de Dados (UNIFACS).

Por força de sua atuação profissional na participação de diversos projetos em várias Organizações, acompanhando o avanço das tecnologias e, igualmente, o avanço dos riscos cibernéticos, trabalhou e liderou iniciativas e projetos com ações de educação em segurança digital para promover o fortalecimento da base de conhecimento das pessoas que trabalhavam nas Organizações e, através destas ações periódicas, foi identificada a redução de incidentes de segurança que envolviam pessoas, após observações dos resultados dos treinamentos em segurança digital. Neste sentido, a pesquisadora, percebeu a necessidade de manter, de forma permanente e periódica, um programa de educação em segurança da informação, englobando também a segurança digital. Este programa passou a fazer parte de sua atuação nas Organizações em que trabalhou.

Esta percepção transformou-se em inquietações pessoais que virou um desejo de contribuir com uma pesquisa na área de educação, sendo possível a investigação de temas como Direitos Humanos, CyberBullying, crimes digitais que afetam a sociedade, além de investigar medidas para o fortalecimento da educação em segurança digital que poderia contribuir para assegurar direitos fundamentais dos indivíduos (incluindo no mundo digital), podendo ser chamados de Direitos Humanos Digitais.

Dentro deste contexto, nasceu a ideia da construção de uma cartilha educativa com dicas e orientações para uso seguro da Internet, com foco em CyberBullying. A cartilha foi chamada de: “Orientações para uma Internet mais humana”, com orientações básicas de segurança digital, sendo possível seu uso para escolas, famílias, profissionais de diversas áreas e, principalmente, para os jovens, indivíduos em formação e grandes vítimas da prática do Bullying e CyberBullying.

Mestrado Profissional do GESTEC

Ressalte-se, aqui, que o Mestrado Profissional “Gestão e Tecnologia Aplicadas à Educação (GESTEC)”, ao qual a pesquisadora está vinculada, é um Programa de Pós-Graduação *Stricto-Sensu* da Universidade do Estado da Bahia (UNEB), vinculado ao Departamento de Educação – DEDC – Campus I. A estrutura, os objetivos e as finalidades do GESTEC orientam-se pela Portaria Normativa nº 17, de 28 de Dezembro de 2009 e Edital nº 005 de 30 de abril de 2010 do Ministério da Educação que dispõem sobre o mestrado profissional no âmbito do sistema nacional de pós-graduação no Brasil. O GESTEC foi aprovado pela Resolução CONSU/UNEB nº 772/2010 e recomendado pela CAPES por meio do ofício nº 039-11/2010/CTC/CAAII/CGAA/DAV/CAPES (UNEB, 2017).

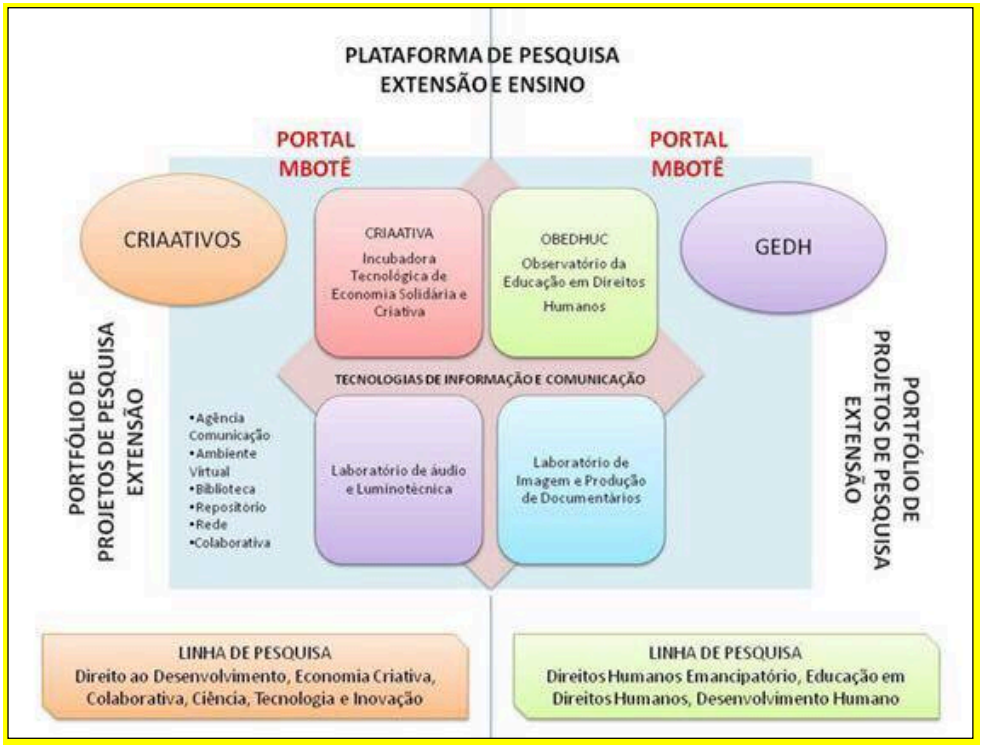
CRDH – Centro de Referência e Desenvolvimento em Humanidades

Atualmente, o “Centro de Referência e Desenvolvimento em Humanidades (CRDH)”, inaugurado em fevereiro de 2017, funciona no bairro do Pelourinho, no centro histórico da cidade do Salvador.

> É um órgão suplementar da Universidade do Estado da Bahia (UNEB), multiusuário, referência em pesquisa, extensão e ensino, com atuação nacional e internacional, e foco na criatividade, ciência, tecnologia e inovação e na capacidade de enfrentar com o conhecimento os desafios impostos à sociedade e ao Estado, principalmente, em relação ao fortalecimento do Estado democrático, cidadania ativa e Direitos Humanos. (CRDH, 2018)

O CRDH possui excelência em pesquisa, extensão, ensino e inovação social e está representado na estrutura, abaixo.

Figura 1. CRDH – Centro de Referência em Desenvolvimento e Humanidades



Autor: Prof. Dr. José Cláudio Rocha (Coordenador do CRDH)

INTRODUÇÃO

A transformação digital promove a digitalização de algumas coisas que antes eram feitas de forma mecânica ou física, como a fotografia, a música ou o até mesmo o uso do papel. Eles migraram dos meios físicos para os meios digitais, quando passaram a ser digitalizados. Já a digitalização gera a desmonetização, pois reduz consideravelmente os custos do que antes existia e era adquirido e consumido em meio físico. A desmonetização, por sua vez, gera democracia, já que mais pessoas podem usufruir, através dos formatos digitais, aquilo que antes somente existia em meio físico, após o surgimento e disseminação das tecnologias de informação e comunicação. Esta transformação digital é um passo importante para a verdadeira inclusão digital e social de pessoas no acesso à informações e serviços que antes eram mais difíceis e custosos por existirem apenas em meios físicos.

Inquestionavelmente estamos vivendo uma nova revolução, a Revolução Digital, que está nos levando a uma nova era: a Era Digital. Os impactos das tecnologias digitais em nossa vida são sem precedentes na história da humanidade, pois, diferentemente de qualquer outra revolução tecnológica do passado, a atual tem causado uma modificação acentuada da velocidade da informação e desenvolvimento tecnológico, acelerando em um ritmo vertiginoso o ambiente em que vivemos. (GABRIEL, 2013, p. 3)

Nesta era digital, a informação é o alicerce da sociedade e é considerada um dos ativos mais valiosos no mundo atual. O fenômeno da globalização, que possibilita a conexão entre indivíduos em qualquer parte do mundo, alicerçado nas diversas tecnologias disponíveis na Internet, trouxe infinitas possibilidades de comunicação.

Pierre Lévy (1999) citou que “A virtualidade, compreendida de forma muito geral, constitui o traço distintivo da nova face da informação”. A partir de determinado momento de evolução das tecnologias de comunicação e informação, a humanidade conhece um novo espaço, o espaço virtual, também conhecido como mundo digital. Mundo esse, habitado pelos mesmos indivíduos que o mundo real, já que são humanos que operam tecnologias.

Hoje, século XXI, o ser humano vive o que se chama de “aldeia global, permitindo que todas as pessoas do mundo possam ter acesso a um fato de modo simultâneo” (PECK, 2016, p 67). Esta aldeia global existe através de conexões digitais feitas a partir de equipamentos e dispositivos capazes de interconectar máquinas e, consequentemente, interconectando os seres humanos, através de dispositivos eletrônicos.

Diante deste cenário, esta pesquisa tem como objetivo geral investigar a importância dos Direitos Humanos no mundo digital da Internet e a aplicação de ações de conscientização em segurança digital, como forma de educar digitalmente para o enfrentamento das práticas do CyberBullying que podem culminar em crimes digitais como racismo, homofobia, entre outros. Aborda, ainda, um estudo sobre direito à privacidade, direito à proteção dos dados pessoais, apresentando e analisando indicadores importantes relacionados a crimes cibernéticos.

A prática do “Cyberbullying” que é o “Bullying Cibernético” ou “Bullying Digital”, é realizada através de equipamentos eletrônicos como o computador ou o celular. Serão explorados e apresentados, nesta pesquisa, conceitos, tipos e agentes do CyberBullying, propondo orientações e dicas de segurança sobre o que fazer, como denunciar e onde buscar ajuda para suas vítimas, a partir da elaboração de uma cartilha orientativa denominada “Orientações para uma Internet mais segura” que contém dicas e recomendações de segurança digital.

Há indícios de problemas graves de saúde mental, casos de suicídio (ou tentativa), em especial, entre jovens, maiores vítimas do Cyberbullying, por não suportarem uma exposição excessiva de suas vidas íntimas ou pessoais, na Internet. Diante disso, é salutar que a sociedade civil tenha conhecimento dos crimes cometidos nos meios digitais, através da Internet, onde ocorrem, seus tipos mais comuns, a gravidade e as consequências geradas em indivíduos vítimas de práticas como o Cyberbullying.

A problemática aqui apresentada é com relação a quais ações devem ser adotadas para fazer com que a sociedade civil esteja informada com relação à prática do Cyberbullying e possíveis crimes digitais que podem derivar do Cyberbullying, além

de informar o que fazer e onde é possível buscar ajuda (no papel de vítima ou testemunha),

O ato de denunciar agressores que praticam um crime digital é um ato corajoso e, acima de tudo, é um ato social. A denúncia, se registrada, aplicada e transcorrida através de um processo jurídico, pode culminar na aplicação de sanções e/ou encarceramento dos agressores, dependendo do tipo e gravidade do ato criminoso. A denúncia de um crime cibernético pode se transformar numa ferramenta e apoio às ações de redução de condutas inadequadas, feitas através das diversas plataformas digitais da Internet.

Ações educativas de conscientização em segurança digital visam promover a disseminação de práticas positivas no uso e cuidados dos espaços digitais na Internet, com instrumentos que ajudem a minimizar a vulnerabilidade digital de indivíduos para que estes, instruídos e capacitados, atentem para os riscos de segurança que estão expostos e também para que possam contribuir com a denúncia de crimes digitais, em caso de serem vítimas ou testemunhas.

A pesquisadora, tendo acompanhado o avanço dos riscos cibernéticos, ao longo de sua trajetória de 30 anos atuando em várias Organizações, pôde identificar a redução de incidentes de segurança nas Organizações em que atuou, em razão das inúmeras campanhas educativas envolvendo as pessoas. Esta percepção transformou-se em inquietações pessoais que se transformaram na iniciativa de fazer pesquisa na área de educação com foco em crimes digitais e na prática do Cyberbullying, visando construção de conteúdos em segurança digital que tivesse alcance social para a sociedade civil.

Assim nasceu a ideia da construção da cartilha educativa “Orientações para uma Internet mais humana”. É importante que a segurança de crianças e adolescentes na Internet e suas inúmeras plataformas digitais e redes sociais seja alvo da atenção de famílias, escolas, Governos e sociedade civil. Esta cartilha orientativa foi pensada como uma forma de contribuir com orientações em segurança digital, numa linguagem simples e de fácil entendimento, para que seja possível seu uso a várias comunidades, escolas, famílias, profissionais de diversas áreas e, principalmente, os jovens.

A cartilha é chamada de “Orientações para uma Internet mais humana” e é produto desta pesquisa. Ela foi construída a partir de uma consolidação de inúmeras fontes de pesquisa, consultadas a partir do levantamento bibliográfico, além de considerar também a experiência da pesquisadora como especialista em segurança digital, conhecedora dos riscos e ameaças cibernéticas que rondam os diversos ambientes e plataformas digitais.

A metodologia utilizada considerou pesquisa bibliográfica para a busca do conhecimento, fontes selecionadas de livros, publicações, sites na Internet (científicos ou não), explorados e considerados como oportunidades de enriquecimento do trabalho. É uma pesquisa aplicada que teve como objetivo gerar conhecimentos para possível solução de problemas específicos e é também exploratória, investigando o tema proposto sob diversos ângulos e aspectos.

1. OBJETIVOS, METODOLOGIA, JUSTIFICATIVA, PROBLEMA DE PESQUISA, HIPÓTESE

1.1 Objetivos

São bem reais as preocupações com os perigos associados ao uso da Internet, seja por parte de adultos, crianças e jovens. Conteúdos impróprios fazem parte deste universo digital, a exemplo daqueles relacionados a pornografia, pornografia infantil, violência, ódio, racismo, que estão facilmente acessíveis, através de uma diversidade de recursos e plataformas digitais, como as redes sociais, jogos online, fóruns, grupos de discussão, entre outros, representando uma verdadeira ameaça.

Crimes digitais praticados na Internet ferem direitos fundamentais dos indivíduos que navegam pela rede, como o direito à privacidade. Práticas como o Cyberbullying (ou Bullying digital) pode oferecer ameaças para aqueles que não podem ou não sabem lidar com este problema. Assegurar os direitos humanos digitais aos indivíduos é fundamental para todos e as ações de conscientização em segurança digital podem ser bastante úteis.

1.1.1 Objetivo Geral

Abordar a importância dos Direitos Humanos no mundo digital da Internet e a aplicação de ações de conscientização em segurança digital para o enfrentamento e alerta de práticas de crimes cibernéticos e do CyberBullying.

1.1.2 Objetivos Específicos

Investigar o tema “Direitos Humanos Digitais”.

Investigar e analisar índices de crimes cibernéticos, em especial aqueles relativos à pornografia infantil, racismo e homofobia.

Investigar o universo que envolve a prática do Cyberbullying.

Estruturar um conjunto de recomendações visando a materialização de uma cartilha de conscientização em segurança digital.

1.2 Metodologia

A busca pelo conhecimento com a exploração de conteúdos é importante para o enriquecimento de pesquisas e o presente trabalho trata-se de uma pesquisa bibliográfica, aplicada e exploratória.

Um trabalho de pesquisa científica envolve tanto o processo de busca de conhecimento quanto o processo de produção do conhecimento. Partindo dessa premissa, a presente pesquisa, quanto aos procedimentos, pode ser classificada como uma pesquisa bibliográfica, ou seja, como o processo de busca do conhecimento, o domínio do estado da arte.

Segundo Marconi e Lakatos (2003, p. 183), a finalidade da pesquisa bibliográfica “é colocar o pesquisador em contato direto com tudo o que foi escrito, dito ou filmado sobre determinado assunto”. No entanto, a velocidade de informações produzidas não nos permite afirmar que o trabalho realizado envolveu tudo que já foi publicado sobre a temática. Principalmente, considerando que não constitui foco desse trabalho campos do conhecimento que tratem do tema cyberbullying na perspectiva da psicologia, das discussões jurídicas das leis apresentadas, da sociologia enquanto busca do entendimento da dinâmica das relações humanas, entre outros.

O foco da discussão proposta se voltou para entender o processo do cyberbullying enquanto produto de uma realidade virtual que possibilita o contato entre comunidades com costumes, valores, ética etc. diferentes, a fim de se apresentar propostas que protejam os “vulneráveis” nesse mundo virtual.

A pesquisa bibliográfica é considerada parte essencial em todo trabalho científico, desde quando coloca o pesquisador diante dos conhecimentos já produzidos e validados no meio acadêmico. Por isso, requer do pesquisador critério para selecionar

o material a ser utilizado especialmente quando nos reportamos às buscas na Internet. Nesta pesquisa, as fontes selecionadas advêm de livros, publicações, sites na Internet, científicos ou não, explorados pela pesquisadora e considerados como oportunidades de enriquecimento do trabalho.

Quanto ao ponto de vista da natureza, trata-se de uma pesquisa aplicada, por ter como objetivo “gerar conhecimentos para aplicação prática dirigidos à solução de problemas específicos. Envolve verdades e interesses locais”. (PRODANOV e FREITAS, 2013, p. 51). A elaboração da cartilha ‘‘Orientações para uma Internet mais humana” constitui a aplicação prática do trabalho proposto, objetivando atender a interesses dos grupos foco do trabalho.

Esta cartilha orientativa foi construída pela pesquisadora e pensada como uma forma de contribuir com dicas e recomendações de segurança digital, numa linguagem de fácil entendimento, possibilitando seu uso nas escolas, famílias, profissionais de diversas áreas e, principalmente, os jovens, indivíduos ainda em formação e grandes vítimas do Cyberbullying. Ela foi concebida a partir de uma consolidação feita pela pesquisadora, a partir de inúmeras fontes de pesquisa, do levantamento bibliográfico, além de considerar também a experiência da pesquisadora como especialista em segurança digital, conhecedora dos riscos e ameaças cibernéticas que rondam os diversos ambientes e plataformas digitais.

Do ponto de vista dos objetivos, a pesquisa pode ser classificada como exploratória, cujo foco é

> proporcionar mais informações sobre o assunto que vamos investigar, possibilitando sua definição e seu delineamento, isto é, facilitar a delimitação do tema da pesquisa; orientar a fixação dos objetivos e a formulação das hipóteses ou descobrir um novo tipo de enfoque para o assunto. [...] A pesquisa exploratória possui planejamento flexível, o que permite o estudo do tema sob diversos ângulos e aspectos. (PRODANOV e FREITAS, 2013, p. 51/52).

Buscamos não só proporcionar mais informações a partir do conhecimento produzido, orientar a fixação dos objetivos e a formulação das hipóteses, mas propor um novo tipo de enfoque para o assunto, principalmente com a análise de exemplos que estimulem a compreensão.

1.3 Justificativa

Em 24 de maio de 1844, Samuel Morse enviava sua primeira mensagem pública por meio de uma linha telegráfica entre Washington e Baltimore, inaugurando com este simples ato a era das telecomunicações (UIT, Nações Unidas). Este fato ocorreu ainda no século XIX.

Hoje, já com os pés no século XXI, o ser humano vive e presencia avanços consideráveis na comunicação, com aparatos tecnológicos capazes de permitir que os indivíduos interajam e se comuniquem, estando as partes em diferentes localidades no mundo.

O movimento de instalar um computador em cada casa, “sai da esteira econômico-corporativa e passa a levar a tecnologia para dentro dos lares, interligando uma rede de consumidores ávidos por informação, serviços e produtos” (PECK, 2016).

O mundo virtual (ou digital), aos poucos, vai se configurando como algo que beneficia a vida dos seres humanos, seja na área de saúde, educação, comunicação, entretenimento, entre outros segmentos.

Esta aldeia global e os aparatos tecnológicos formam o que se conhece como “Internet” que é uma rede de computadores que trocam dados e informações, proporcionando a interação quase instantânea entre seres humanos, como define Cassanti (2014, p.1):

> “A Internet é um conjunto de redes de comunicação em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de

> comunicação TCP/IP, que permite o acesso a informações de todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que, como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores".

Em recente pesquisa, a União Internacional de Telecomunicações (UIT, 2018, S/P), Agência do Sistema das Nações Unidas dedicada a temas relacionados às Tecnologias da Informação e Comunicação (TICs), divulgou que a penetração da Internet, no mundo, é de 81% nos países desenvolvidos, de 40% nos emergentes e de 15% nos países mais pobres. O percentual de indivíduos utilizando a Internet é de 79,1% na Europa e de 65% nas Américas. Os indicadores caem na Ásia/Pacífico, que tem 41,9%; nos Estados Árabes, com 41,6%; e na África, que tem o menor indicador mundial, com 25,1%.

Através deste recorte de dados, percebe-se, nos dias de hoje, o grande alcance da Internet no mundo, apesar de ainda ser muito mais nos países desenvolvidos, em função da necessidade de investimentos para aquisição e uso dos equipamentos que promovem o funcionamento e operacionalização das redes de computadores que constroem e mantêm a Internet.

Estamos falando não apenas de uma comunidade virtual, mas de várias comunidades virtuais que se aglomeram em torno de objetivos comuns, várias tribos com participantes de vários pontos do planeta, de diversas culturas, sujeitos cada um a princípios de valor e normas distintas (PECK, 2016, p. 69). Indivíduos de culturas diferentes que se beneficiam do aprendizado de novos saberes, do compartilhamento de experiências, da distribuição de conhecimentos.

Ainda sob a abordagem relacionada à Internet, Gabriel (2013, IX) cita que

> Em pouco mais de uma década, vimos a Internet tornar-se a principal plataforma planetária de comunicação, entretenimento, negócios, relacionamento, aprendizagem e a infraestrutura responsável pelo novo tecido da humanidade globalizada. Esse cenário é deslumbrante e transforma a web no cérebro global conectado, onipresente, onisciente e onipotente. No entanto, esse novo panorama repleto de possibilidades, conexões e

> ampliação do potencial humano traz também consigo profundas transformações e, consequentemente, novos desafios.

Portanto, são muitos os desafios em termos de tecnologia, cultura, educação e possibilidades de comunicação. Segundo dados do Worldometers[1] (2018) a Internet, atualmente, já passou dos 4 bilhões de usuários no mundo, diariamente são enviados mais de 200 bilhões de e-mails por dia, mais de 5 bilhões de buscas são feitas diariamente no Google[2]. Estes são apenas alguns números para se ter a dimensão da Internet e da massa de dados e informações que são trafegadas todos os dias, a todo o momento.

São milhões de indivíduos acessando, postando, se comunicando e compartilhando ideias, pesquisas e vidas, através de sites, blogs, redes sociais, jogos online e plataformas digitais disponíveis a um "clique".

Assim como o mundo digital proporciona tantos benefícios, ameaças e riscos de segurança fazem parte desta Internet de bilhões de usuários, criando preocupações com uso de equipamentos e dispositivos conectados à Internet. Acessar, postar, expor, inferir, criticar, agredir, difamar, violar são algumas das ações praticadas diariamente por milhões de indivíduos conectados através dos diversos espaços virtuais existentes atualmente.

Serão apresentados alguns índices relacionados a crimes de racismo, pornografia infantil e homofobia nesta pesquisa, além da investigação sobre a prática do Cyberbullying que poder ser um instrumento condutor de um crime na Internet.

1.4 Problema de Pesquisa

Há indícios de casos de morte e suicídio, em especial, entre jovens, vítimas de Cyberbullying, por não suportarem uma exposição excessiva de suas vidas íntimas ou pessoais, na Internet. É salutar que a sociedade civil seja e esteja informada sobre

[1] Site administrado por uma equipe internacional de desenvolvedores, pesquisadores e voluntários com o objetivo de disponibilizar estatísticas mundiais relacionadas a vários segmentos da vida no planeta Terra.
[2] Site de busca na Internet.

crimes cometidos nos meios digitais, através da Internet, onde ocorrem, seus tipos mais comuns, a gravidade e as consequências geradas em indivíduos vítimas de práticas como o cyberbullying.

Mas para que a sociedade civil se informe, questiona-se: Quais ações devem adotar? O que fazer? Onde buscar ajuda quando se depararem com casos de crimes digitais, sendo vítima ou testemunha de um crime?

1.5 Hipótese

Analogamente à vida física e real, a promoção de uma cultura de respeito e valorização dos Direitos Humanos no mundo digital, através de ações de educação e segurança digital para a sociedade civil, podem colaborar no combate à criminalidade digital, em especial, no enfrentamento às práticas do cyberbullying (ou bullying digital) e, quem sabe até, contribuir para a redução dos índices de mortes entre jovens.

2. CONTEXTUALIZAÇÃO TEÓRICA: DIREITOS HUMANOS, DIREITOS HUMANOS DIGITAIS, BULLYING, CYBERBULLYING E CRIMES DIGITAIS.

2.1 Direitos Humanos e Direitos Humanos Digitais

Neste ano de 2018, em que a “Declaração Universal de Direitos Humanos” (DUDH) completa 70 anos, diversos países do mundo estão realizando campanhas para reforçar os direitos humanos fundamentais de qualquer ser humano habitante deste planeta.

> O conceito de direitos humanos é uma pedra angular de nossa humanidade. Tais direitos não são concedidos porque somos cidadãos de uma nação, mas porque são direitos de toda a humanidade independente de qualquer distinção. O conceito de direitos humanos universais é, desse ponto de vista, uma ideia unificadora, algo que torna cada um de nós importante (pouco importa onde vivamos e a que país pertençamos), algo que podemos todos partilhar (apesar da diversidade dos sistemas jurídicos dos nossos respectivos países). Os direitos humanos não são frutos de um país ou de um povo. Eles são concebidos pela humanidade para toda a humanidade. (ROCHA, 2014)

Como bem expressado nesta afirmação de ROCHA (2014), os direitos humanos são direitos inerentes a todos os seres humanos, independentemente de raça, sexo, nacionalidade, etnia, idioma, religião ou qualquer outra condição.

Os direitos humanos são garantidos pela lei de direitos humanos, protegendo indivíduos e grupos contra ações que podem interferir nas liberdades fundamentais dos seres humanos.

Algumas características importantes dos direitos humanos: eles são fundados sobre o respeito pela dignidade e o valor de cada pessoa; são universais, ou seja, são aplicados de forma igual e sem discriminação; são inalienáveis, e ninguém pode ser privado de seus direitos humanos; são indivisíveis, inter-relacionados e interdependentes.

O conhecimento do espaço digital da Internet e seus diversos recursos e aparatos tecnológicos é significante, considerando que esta ambientação digital servirá para o

entendimento acerca de crimes digitais, segurança digital e Direitos Humanos Digitais, objetos desta pesquisa.

Todo ser humano deve ter os seus direitos humanos assegurados e respeitados. Estes mesmos direitos devem ser respeitados no mundo digital, neste mundo que podemos também chamar de Internet. “As novas tecnologias da informação estão integrando o mundo em redes globais de instrumentalidade. A comunicação mediada por computadores gera uma gama enorme de comunidades virtuais”. CASTELLS (2016, p. 77)

Os Direitos Humanos diferem dos Direitos Humanos Digitais em função do espaço em que ele é exercido e respeitado. Enquanto o primeiro é exercido na vida física e real que vivemos, o segundo é exercido nos espaços digitais da Internet, sejam em redes sociais, sites, blogs, jogos, comunidades virtuais em geral, todos, todos eles devem respeitar igualmente os direitos fundamentais de qualquer pessoa que seja usuária de ambientes virtuais. Nesse sentido, o direito à “Privacidade” implica no fato de que “Privacidade deriva do latim (*privatus*) e significa ‘separado do resto’. De mais amplo, refere-se à habilidade dos indivíduos (ou grupos) de afastar a si próprios e, consequentemente, revelar apenas as suas informações que deseje, de modo seletivo”. (GABRIEL, 2018, p. 62).

Privacidade é um direito humano fundamental. Está referenciada na DUDH em seu artigo XII que diz: “Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.” (ONUBR, 2018, S/P).

Privacidade é um direito constitucional brasileiro. Está referenciada na Constituição da República Federativa Brasileira, datada de 1988, em seu artigo 5º, inciso X, que diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação.” (BRASIL, 2016, p. 13).

Privacidade é referenciada na Lei 12.965/2014, também conhecida como “Marco Civil da Internet” que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Em seu artigo 10º. Ela cita

> “A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas”. BRASIL, 2014, p. 5).

Privacidade também é referenciada nos “Princípios para a Governança e Uso da Internet no Brasil”, em seu artigo 1º que diz “O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática”. (CGI.BR, 2009, p. 1).

Privacidade também está referenciada na recente Lei 13.709/2018, mais conhecida como “Lei Geral de Proteção de Dados”, em seu artigo 1º que diz

> “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, p. 1).

No contexto apresentado, percebe-se que o direito à privacidade é um direito humano, é um direito constitucional e um direito humano digital. Ele deve ser respeitado e assegurado na vida física real, assim como na vida digital da Internet. A privacidade é um direito seletivo para revelar informações pessoais, desde que declarado o consentimento pelo seu titular.

Nos ambientes digitais, em que as informações são disseminadas de forma exponencial, onde milhares ou até milhões de pessoas passam a conhecer um fato ou informação em poucos minutos, através da Internet, é cada vez mais imprescindível o cuidado com os dados pessoais, sejam pelo lado de seus titulares, expondo somente aquilo que é necessário nos ambientes digitais, seja pelo lado das organizações que, hoje, em função da legislação vigente, a exemplo da “Lei Geral de

Proteção de Dados" (LGPD), deve, obrigatoriamente, utilizar dados de usuários e consumidores, apenas para a finalidade devida e consentida pelo seu titular.

A globalização é o processo pelo qual determinada condição ou entidade local estende a sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival (SANTOS, 2013). Observa-se o papel fundamental das tecnologias da informação e comunicação ao que hoje entende-se estar num mundo globalizado.

Inquestionavelmente estamos vivendo uma nova revolução, a Revolução Digital, que está nos levando a uma nova era: a Era Digital. Os impactos das tecnologias digitais em nossa vida são sem precedentes na história da humanidade, pois, diferentemente de qualquer outra revolução tecnológica do passado, a atual tem causado modificação acentuada da velocidade da informação e desenvolvimento tecnológico acelerando em um ritmo vertiginoso o ambiente em que vivemos (GABRIEL, 2013).

A sociedade é digital, o mundo está globalizado, as comunidades são virtuais, as tecnologias da informação e comunicação são indispensáveis para essa engrenagem funcionar. Indivíduos são atores que mantêm infraestruturas, mas que também as utilizam nas diversas formas materializadas.

"O futuro nunca esteve tão colado ao presente. Nada pode ser reclamado em nome do futuro que não tenha um nome e um sentido para os que vivem hoje e podem não estar vivos amanhã" (SANTOS, 2013, p. 123). Já vivemos hoje num mundo que, até alguns anos atrás, considerava-se como futurista. Já existem hoje tecnologias disponíveis às pessoas comuns que alteram, significativamente, o modo como elas vivem, trabalham, comunicam-se, relacionam-se, aprendem.

> "As novas tecnologias não afetam apenas o modo como fazemos as coisas, mas afetam principalmente nossos modelos e paradigmas – as regras intrínsecas de como as coisas deveriam ser -, e é de se esperar que, nesta nova estrutura sociotecnológica, as expectativas e os relacionamentos educacionais sofram as mesmas modificações significativas e perceptíveis que têm ocorrido em nossas vidas cotidianas" (GABRIEL, 2013, p. 7).

Reconhecer a cibersegurança (ou segurança digital) será uma tarefa desafiadora, a demandar uma série de esforços (tecnológicos, financeiros, econômicos, jurídicos, entre outros), para que seja possível reconhecer esta matéria, visando a almejada "paz na rede", conforme preconizado por Schackelford (2017), como 2º passo para que a Internet seja um ambiente menos inóspito, cruel e temeroso. O 1º passo já será demasiado desafiador, tornando o acesso à Internet um direito humano, visando a liberdade de expressão, de manifestação e de troca de informação, considerando a parcela mundial conectada à grande rede, através dos mais variados dispositivos.

Mesmo se considerarmos um mundo digital mais seguro e com menos riscos de ameaças digitais, as redes sociais não estariam livres de ameaças. Daí a importância da educação e ações de conscientização em segurança digital que possam servir de apoio e ferramenta para minimizar a vulnerabilidade digital dos indivíduos, servindo também como suporte para o enfrentamento dos crimes digitais.

Sobre esta temática, o Governo Federal Brasileiro instituiu, em 2015, o "Programa de Combate à Intimidação Sistemática (Bullying)", através da Lei 13.185, onde, na mesma esteira, trata do *bullying* no meio digital, quando

> "Há intimidação sistemática na rede mundial de computadores (cyberbullying), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial." (BRASIL, 2015, S/P).

Esta Lei tipifica o bullying e cyberbullying como práticas inadequadas, porém, não criminaliza suas ações. A consequência dos atos destas práticas é que podem ser consideradas crimes, a exemplo de calúnia, difamação e injúria que serão abordados e detalhados em capítulo específico.

Os desafios são inúmeros. Não é suficiente pensar em promover a distribuição de ativos tecnológicos (computadores, tablets, smartphones, etc) sem, ao menos, pensar em promover um mínimo de conhecimento técnico do mundo digital a ser consumido e utilizado.

> "O acesso ao ciberespaço exige infraestruturas de comunicação e de cálculo (computadores) de custo alto para as regiões em desenvolvimento. [...] É preciso ainda superar os obstáculos 'humanos'. Em primeiro lugar há os freios institucionais, políticos e culturais para formas de comunicação comunitárias, transversais e interativas. Há, em seguida, os sentimentos de incompetência e de desqualificação frente às novas tecnologias." LÉVY (1999, p. 235 e 236).

Seguindo este pensamento, fornecer apenas tecnologia "não assistida", com inexistência de conhecimento prévio do que será utilizado, qual deve ser a melhor forma de utilizar uma tecnologia e, em especial, quais os riscos existentes e inerentes nesta tecnologia, pode não resolver a questão da necessidade de acesso dos indivíduos à Internet, às redes sociais.

Pode-se pensar, metaforicamente, que seria o mesmo que fornecer acesso a um carro para um indivíduo e não o ensinar a dirigir, não apresentar ou dar ciência sobre as leis de trânsito, principalmente considerando que, na "rua digital" que é a Internet, o acesso é feito por indivíduos de diferentes países, raças, culturas e tradições...todos podem estar juntos numa mesma via de acesso digital.

É possível que o Brasil esteja diante de uma oportunidade de evolução no quesito "aprendizagem em novos conteúdos tecnológicos", inclusive para indivíduos cada vez com menos idade acessando Internet, redes sociais e o mundo digital que os rodeia. Nos dias de hoje, crianças chegam nas escolas para serem alfabetizadas, já com uma carga horária razoável de uso de redes sociais.

> "Quando falamos da emergência de múltiplos paradigmas, é sinal de que precisamos rever, olhar de outro jeito e alterar o modo como fazemos e pensamos as coisas, como refletimos sobre a nossa prática dentro da Educação. [...]. Se os alunos não são mais os mesmos, se o mundo não é mais o mesmo, como fazer do mesmo modo? Há alguns aspectos na área da Educação que precisam ter uma durabilidade maior, mas há algo de que não podemos esquecer: a importância de olhar a realidade; porque, afinal de contas, a Educação lida com o futuro" (CORTELLA, 2014, p. 9 e 10).

"A tecnologia em si não é um direito, mas um meio através do qual direitos podem ser exercidos", cita CERF (2012, S/P) considerado por muitos como o "pai" da Internet. Nesse artigo publicado no jornal "The New York Times", em janeiro de 2012, intitulado: "Acesso à Internet não é um direito humano", ele faz considerações importantes a

respeito das tecnologias e suas representações enquanto direitos civis e direitos humanos. Em seu texto, ele comenta “Na verdade, mesmo o relatório das Nações Unidas, que foi amplamente saudado como declarando o acesso à Internet um direito humano, reconheceu que a Internet era valiosa como um meio para um fim, não como um fim em si mesmo”.

E segue afirmando “A Internet introduziu uma plataforma enormemente acessível e igualitária para criar, compartilhar e obter informações em uma escala global. Como resultado, temos novas maneiras de permitir que as pessoas exerçam seus direitos humanos e civis”. CERF (2012, S/P) ainda afirma “Melhorar a Internet é apenas um meio, embora importante, para melhorar a condição humana. Deve ser feito com uma apreciação pelos direitos civis e humanos que merecem proteção - sem fingir que o acesso em si é um tal direito”.

A sociedade digital em que se vive hoje, com uso massivo das inúmeras tecnologias para acesso às redes sociais, as quais promovem conexão e comunicação entre indivíduos, necessita o delineamento de estruturas formais que definam uso e direitos na Internet.

FIORILLO (2015) articula, em sua obra, comentários sobre todos os artigos da Lei 12.965/2014, reforçando a necessidade da manutenibilidade dos direitos e deveres fundamentais dos indivíduos (tal qual já expressamente abordados na Constituição Brasileira (1988), explica que:

> “O denominado Marco Civil da Internet (Lei 12.965/2014), ao pretender estabelecer princípios, garantias, direitos e deveres vinculados à manifestação do pensamento, à criação, à expressão e à informação (meio ambiente cultural), por meio do uso da Internet no Brasil (meio ambiente digital), procura de qualquer forma tentar organizar parâmetros jurídicos específicos no âmbito infraconstitucional destinados a tutelar o conteúdo da comunicação social e mesmo dos direitos e deveres fundamentais da pessoa humana por meio do uso de computadores no Brasil em redes interligadas, visando, ao que tudo indica, destacar a importância da tutela jurídica da Internet do século XXI em nosso País.
>
> [...] o uso da Internet no Brasil, a partir da presente Lei n. 12.965/2014, deve sempre ser preliminarmente interpretado em face dos princípios fundamentais de nossa Constituição Federal, que enquadra a ordem econômica do capitalismo bem como o meio ambiente cultural

> necessariamente em face da dignidade da pessoa humana". (FIORILLO, 2015)

Pensando na sociedade digital e considerando que estes fatores coexistem no mundo digital da Internet, paralelamente, os artigos da "Declaração Universal dos Direitos Humanos" caberiam em "qualquer dos mundos" (o real e o digital). Neste caso, importa o direito, não o meio em que ele vai coexistir.

O que seria a "segurança pessoal" no mundo digital, senão, as tratativas computacionais derivadas de extensas redes de conexão para processar, armazenar e promover a comunicação e conexão entre povos, entre indivíduos, entre nações e, atualmente, até entre o planeta Terra e astronautas no espaço.

Além do aparato tecnológico precisar estar em constante processo de monitoramento, através das diversas ferramentas de segurança cibernética para promover a proteção das redes de informação, é importante considerar também o aspecto relativo ao conhecimento tácito que cada indivíduo possui relativo ao uso da Internet e das redes sociais; seus riscos, benefícios e forma de manuseio, porque a vida e a segurança pessoal andam ameaçadas no mundo digital.

Se o Conselho de Direitos Humanos das Nações Unidas entende que direitos humanos valem tanto *online* quanto *offline*, pode-se perceber o urgenciamento no tratamento das questões inerentes aos direitos humanos, como direito à privacidade, direito à proteção de dados pessoais, combate ao *cyberbullying,* combate ao racismo, homofobia, entre outros.

A Assembleia Geral das Nações Unidas reforça o "direito à privacidade na era digital", fato abordado no período das inúmeras revelações sobre espionagem eletrônica dos EUA em todo o mundo, no ano de 2014.

> Governos do mundo inteiro têm se esforçado fortemente para treinar seus cidadãos a desdenhar a própria privacidade. Uma ladainha de lugares-comuns hoje conhecidos de todos convenceu as pessoas a tolerarem invasões brutais a seu universo privado: as justificativas foram tão bem sucedidas que muitos aplaudem enquanto as autoridades coletam grandes quantidades de informação sobre o que dizem, leem, compram e fazem – e com quem. (GREENWALD, 2014, p. 183)

O acesso à Internet deverá se tornar reconhecido como um direito humano. A segurança digital deverá (ou poderá) “vir à galope”, com vias digitais mais “limpas”, com menos riscos, principalmente para os “pilotos de 1ª viagem”, aqueles que ainda não possuem maturidade e experiência para lidar com um mundo de imperfeições.

“Os smartphones estão se tornando o controle remoto do mundo” (MELLO, 2017). Com base nos dados da pesquisa do IBGE, esta frase de MELLO é bem atual. *Smartphones* ou celulares inteligentes em mãos de indivíduos realizando uma infinidade de tarefas diariamente, através destas tecnologias: compram, vendem, jogam, comunicam-se, aprendem, assistem e, é claro, fotografam e filmam a vida a seu redor. Estas últimas ações tornam os smartphones como observatórios e “controles remoto” do mundo.

A Internet e a infinidade de redes sociais à disposição dos indivíduos no mundo digital possui um “lado positivo” de incontáveis benefícios do uso da tecnologia para o cidadão. Do mesmo modo, há um “lado negativo”, ameaçador, cheio de riscos, ilusões, o verdadeiro e o falso se confundem. Perfis falsos, informações falsas, relacionamentos falsos, amizades e propostas falsas, enfim, cada um com suas especificidades. Até porque,

> Seria preciso ensinar princípios de estratégia que permitissem enfrentar os imprevistos, o inesperado e a incerteza, e modificar seu desenvolvimento, em virtude das informações adquiridas ao longo do tempo. É preciso aprender a navegar em oceanos de incerteza em meio a arquipélagos de certeza (MORIN, 2011, p.17).

Utilizando a metáfora “aprender a navegar em oceanos de incerteza”, citada acima por MORIN, comparando aos inúmeros ambientes virtuais que existem na Internet, dos quais, a juventude navega, considerando que não se conhecem as identidades reais de seus usuários e considerando a diversidade de ambientes existentes, vê-se a importância de “ensinar princípios de estratégia que permitissem enfrentar os imprevistos, o inesperado e a incerteza, e modificar seu desenvolvimento”, criando uma consciência diferenciada acerca do mundo digital, suas ameaças e riscos

potenciais, através de conteúdos educacionais específicos para suas respectivas faixas etárias.

“As mudanças são tão profundas que, na perspectiva da história humana, nunca houve um momento tão potencialmente promissor ou perigoso”. (SCHWAB 2016, p. 12).

“A tecnologia não é uma força externa, sobre a qual não temos nenhum controle. Não estamos limitados por uma escolha binária entre ‘aceitar e viver com ela’ ou ‘rejeitar e viver sem ela’. Na verdade, tomamos a dramática mudança tecnológica como um convite para refletirmos sobre quem somos e como vemos o mundo.” (Schwab 2016, p. 13).

Neste capítulo serão abordadas questões relacionadas ao bullying, cyberbullying e crimes digitais ou crimes cibernéticos que são aqueles praticados através do uso das tecnologias disponíveis atualmente.

2.2 Bullying

O bullying não possui tradução específica, mas seria algo parecido como uma intimidação, um desejo consciente e deliberado de maltratar alguém, colocando-a sob um estado de tensão que pode provocar até danos psicológicos na vítima que sofrem humilhações onde, em muitos casos, ficam com a auto-estima baixa.

> Todos os dias, alunos do mundo todo sofrem com um tipo de violência que vem mascarada na forma de “brincadeira”. Estudos recentes revelam que esse comportamento, que até bem pouco tempo era considerado inofensivo e que recebe o nome de bullying, pode acarretar sérias consequências ao desenvolvimento psíquico dos alunos, gerando desde queda na auto-estima até, em casos maios extremos, o suicídio e outras tragédias. (PARAÍBA, 2009, p. 3)

A Promotoria da Infância e Juventude pertencente ao Ministério Público do Estado da Paraíba aborda, acima, sobre consequências para as vítimas do bullying. Elas são imprevisíveis, bem diversas, depende das reações de cada indivíduo, desde

isolamento, agressões, homicídios e até tentativas de suicídio. A Promotoria ainda explana considerações acerca do Bullying, conforme segue:

> "Bullying é uma palavra de origem inglesa, que não tem uma tradução em português, utilizada em muitos países para descrever atos de violência física ou psicológica, intencionais e repetidos, sem motivação evidente, praticados por uma ou mais pessoas contra outra (s), causando dor e angústia, dentro de uma relação desigual de poder, tornando possível a intimidação da vítima" (PARAÍBA, 2009, p. 5)

No mesmo contexto do bullying e suas práticas de intimidação constante, existe a prática do cyberbullying, também conhecido como bullying cibernético. São as intimidações praticadas com uso de tecnologias, realizadas de diversas formas e que causar prejudicar suas vítimas de forma mais ampla e agressiva, considerando as possibilidades de disseminação destas práticas, através das diversas e inúmeras plataformas digitais.

Como ressalta Silva (2015, p. 14) "De forma quase 'natural', os mais fortes utilizam os mais frágeis como meros objetos de diversão, prazer e poder, com o intuito de maltratar, intimidar, humilhar e amedrontar suas vítimas". Seja no mundo físico ou digital, a educação pode ser o veículo para levar informações e orientações a respeito do tema, com foco a todos os envolvidos neste tipo de prática (agressores, vítimas e testemunhas).

Silva (2015, p. 21) acrescenta ainda que

> o bullying pode acontecer de forma direta ou indireta. Porém, dificilmente a vítima recebe apenas um tipo de agressão; normalmente, os comportamentos desrespeitosos dos 'bullies' costumam vir em bando. Essas atitudes maldosas contribuem não somente para a exclusão social da vítima, como também para muitos casos de evasão escolar e pode se expressar das mais variadas formas.

Os avanços tecnológicos e o uso, cada vez mais intenso, das inúmeras plataformas digitais disponíveis aos usuários da Internet, possibilitaram o surgimento de novas formas de bullying. Silva (2015, p. 32) segue abordando que "talvez o maior desafio na identificação dos atores dessa triste peça chamada bullying seja distinguir os

agressores que podem ser dissuadidos desse papel daqueles que já exibem, desde muito cedo, uma natureza desprovida de afetividade.”

O item a seguir explora a prática do cyberbullying (bullying cibernético, praticado no mundo digital), sua conceituação, tipos de práticas, agentes envolvidos e conteúdos explorados no tema.

2.3 Cyberbullying

O cyberbullying é um problema mundial, muitas vezes subestimado por muitas pessoas que consideram se tratar apenas de uma brincadeira de crianças. Ciberbullying não é brincadeira. Só existe brincadeira quando todos os envolvidos se divertem. Quando há uma relação desigual de poder, onde uns se divertem e outros sofrem e são maltratados, então é preciso que os adultos tomem uma providência.

Cassanti (2014, p. 35) define cyberbullying como “a ação intencional de alguém fazer uso das tecnologias de informação e comunicação (TICs) para hostilizar, denegrir, diminuir a honra ou reprimir consecutivamente uma pessoa”.

Dentro do mesmo contexto, Rocha (2012, p.82) define o cyberbullying como:

> um modo dissimulado de agressão, por ser oral e escrita. Os agressores intimidam suas vítimas através de dois meios – o computador e o celular. [...]. A mobilidade das tecnologias digitais tira o sossego das vítimas, o que faz do cyberbullying uma forma de violência invasiva que ameaça os indivíduos em diferentes locais.

Um outro autor, Santana (2013, p. 69), define o cyberbullying como “uma extensão do bullying, via Internet e/ou telefone celular”. Complementa citando o cyberbullying como bullying eletrônico, digital ou virtual.

Estas conceituações, acima, destacam os aspectos repetitivos, similares ao bullying, além dos aspectos intencionais e ofensivos.

O Ciberbullying, como modalidade virtual do bullying, conforme definições de Cassanti (2014, p. 35), Rocha (2012, p.82) e Santana (2013, p. 69), é identificado pelas intimidações repetitivas, muito comum entre crianças e adolescente e tem um efeito exponencialmente multiplicador e de grandes proporções, em função dele ocorrer no mundo digital.

Ainda a respeito do entendimento sobre o cyberbullying, Silva (2015, p.134) explana que “os praticantes de cyberbullying, ou ‘bullying virtual’, utilizam os mais atuais e modernos instrumentos da Internet e de outros avanços tecnológicos na área da informação e comunicação (fixa ou móvel) com o covarde intuito de constranger, humilhar e maltratar suas vítimas”.

Informar e orientar sobre o que é o cyberbullying e, de certa forma, como se proteger no mundo virtual, é importante para entendimento sobre o assunto a todos os atores envolvidos, crianças, adolescentes, adultos etc.

É importante identificar se uma criança ou adolescente está sofrendo casos de agressão repetitiva através da Internet, o ciberbullying. É importante verificar mudanças de comportamento e alterações de humor.

Silva (2015, p. 134 e 135) ainda inclui a questão do anonimato como fator que dificulta a identificação dos praticantes do cyberbullying, facilitando a prática de seus algozes. Neste aspecto, ela cita que

> No caso do cyberbullying, a natureza vil de seus idealizadores e/ou executores ganha uma ‘blindagem’ poderosa pela garantia do anonimato que eles adquirem. Sem nenhum tipo de constrangimento, os bullies cibernéticos (ou virtuais) se valem de apelidos (nicknames ou simplesmente nicks) ou perfis falsos com o nome de outras pessoas conhecidas ou de personagens famosos de filmes, novelas, seriados. Os bullies virtuais são, a meu ver, os verdadeiros covardes mascarados de valentões, que se escondem nas redes de ‘esgoto’ do universo fantástico dos grandes avanços tecnológicos da humanidade.

Há indícios que podem revelar que a criança ou adolescente está sendo vítima de cyberbullying. Algumas delas podem ser identificadas, como mudanças repentinas no uso da Internet, medo de compartilhar o que faz na Internet, medo de ir para a escola

e encontrar amigos, evitar participar de atividades coletivas, sinais incomuns de tristeza e isolamento no intervalo da escola. (Safernet)

“Todos podem se tornar vítimas de um bombardeio maciço de ofensas, que se multiplicam e se intensificam de forma veloz e instantânea quando disparadas via celular e Internet”. Este ponto abordado por Silva (2015, p. 136) expressa a intensidade na disseminação da prática do cyberbullying com uso das plataformas digitais à disposição de seus usuários.

A Safernet (S/D) apresenta algumas características importantes do cyberbullying que valem a pena ser destacados:

a) O Cyberbullying se caracteriza pelo ato de insultar, humilhar e praticar violência psicológica repetitiva e persistente, provocando intimidação e constrangimento de crianças e adolescentes através da Internet o dos dispositivos móveis.

b) Em razão das particularidades das interações virtuais, o cyberbullying pode ser um ato difícil de cessar e parece não ter fim. Em ambientes offline é possível controlar e cessar a violência no momento em que acontece. Em ambientes online o alvo está constantemente exposto a ela, mesmo que mude de endereço, escola ou cidade, a violência tende a persistir.

c) Pode ser invisível para adultos e educadores, por acontecer em ambientes onde nem sempre há a presença de adultos.

d) É a principal preocupação de crianças e adolescentes. Mas os adultos tendem a subestimar sua importância, encarando o cyberbullying como uma brincadeira de crianças, sem gravidade.

e) O cyberbullying não é uma brincadeira, e sim uma forma de uma criança ou adolescente demonstrar poder sobre as outras.

f) Cyberbullying não é brincadeira porque só existe brincadeira quando todos os envolvidos se divertem. Quando há uma relação desigual de poder, onde uns

se divertem, enquanto outros sofrem e são maltratados, então é preciso que os adultos intervenham.

A mídia, vez por outra, apresenta casos reais de suicídio entre jovens, vítimas de cyberbullying. Alguns casos que exemplificam isso são relatados abaixo, o que demonstra o poder devastador de atitudes agressivas, ofensivas, embaladas de ódio e violência repetidamente feitas por agressores a pessoas, na maioria das vezes, jovens que se sentem carentes, indefesos, com suas vidas expostas através da Internet e que, infelizmente, na maioria dos casos, acabam tirando suas próprias vidas por não suportarem tanta pressão. Alguns casos divulgados livremente na Internet:

- O famoso caso da ex-estagiária da Casa Branca (Estados Unidos), Monica Lewinski, e seu envolvimento com o então Presidente Bill Clinton. Muitos anos após os escândalos midiáticos, a própria Monica aborda o terror que ela viveu, através de um TED Talk (YOUTUBE, S/D), abordando o poder devastador que a Internet pode provocar na vida de uma pessoa. Este, inclusive, foi considerado um dos primeiros casos de cyberbullying no mundo.

- O caso da garota canadense que em 2014 suicidou-se por não ter suportado meses de assédio e ofensas pela Internet, após ter sido estuprada (BBC, S/D).

- O caso do brasileiro que perdeu peso e postou fotos comparativas do “antes” e “depois” de seu processo de emagrecimento, foi agredido nas redes sociais pelas fotos publicadas (G1, S/D).

- O caso da canadense que suicidou-se em 2012, após sucessivas agressões em redes sociais (TECHNOBLOG, S/D).

- O caso da adolescente que se matou, após sofrer sucessivas agressões virtuais. Vítima de cyberbullying (SAFERNET, S/D).

- Um resumo de casos relatados de bullying e cyberbullying que tiveram finais trágicos de suas vítimas expostas ao terror nas redes sociais ou mesmo na vida real (IEFAP, S/D).

Ao aprofundar no tema, é possível perceber o caos que as vidas destas e outras tantas pessoas se transformam, em função das agressões sucessivas, sejam na vida real (bullying) ou na vida digital (cyberbullying). Não se trata de brincadeira entre jovens nas escolas, o problema é muito maior. No caso do cyberbullying, inclusive, o problema ultrapassa as fronteiras físicas da escola, pois há casos em que os agressores são de outras cidades e até de outros países, visto que as agressões são feitas por redes sociais na Internet.

Ações educativas de conscientização sobre o que é o cyberbullying, o que deve ser feito, a quem deve-se buscar ajuda, são importantes para o esclarecimento sobre este fenômeno. É importante que o futuro seja construído hoje, a partir de ações realizadas que visem o aprimoramento da ética e da segurança na Internet. A Safernet (S/D) comenta que

> O futuro da internet depende do que se faz com ela hoje. Ao usar a internet para agredir e humilhar alguém há um estímulo para que novas leis de controle e proibição sejam criadas e quem perde são os internautas, que tem sua liberdade cada vez mais vigiada e cerceada pelo comportamento de uma parte da sociedade.

A conduta jurídica do cyberbullying, depende da jurisdição de cada país. Conforme comenta Silva (2015, p. 153),

> No Brasil, caso o cyberbullying seja praticado por maiores de idade e configure crime, cabem ação penal privada (por exemplo, para processar criminalmente o agressor que pratique crimes contra honra, como calúnia, difamação e injúria) e ação penal pública (para processar criminalmente o agressor que pratique o crime de ameaça, por exemplo). Entretanto, se as condutas forem praticadas por menores de dezoito anos, caberá ao Ministério Público (com atribuição na Vara da Infância e da Juventude) pleitear ao juiz competente a apuração do ato infracional.

Algumas dessas práticas criminosas, que podem ser praticadas através do Cyberbullying, possuem as seguintes características:

A) Calúnia – alguém imputando falsamente fato definido como crime. Pena: detenção, de seis meses a 2 anos e multa

B) Difamação – alguém imputando fato ofensivo à sua reputação. Pena: detenção, de 3 meses a 1 ano e multa

C) Injúria – alguém ofendendo a dignidade ou decoro. Pena: detenção, de 1 a 6 meses ou multa

À medida que a conscientização sobre este fenômeno se amplia, vítimas, familiares e amigos de vítimas têm procurado a Justiça para divulgação de casos reais, visando registro e providências cabíveis.

Silva (2015, p. 54) aborda que “auxiliar e conduzir as novas gerações na construção futura de uma humanidade mais justa e menos violenta são um imperativo categórico de que todos nós deveríamos nos incumbir”.

Coordenar ações de sensibilização, com orientações consistentes e uso seguro de plataformas e ambientes digitais pode ser um componente importante e agregador para jovens, famílias, escolas e sociedade civil, diante do enfrentamento e proteção às práticas utilizadas pelo cyberbullying.

As consequências causadas pela prática do cyberbullying podem ser diversas e bem complexas. Sobre este ponto, Silva (2015, p. 137) aborda que

> quando as vítimas se deparam com toda essa gama de maldades maquiavelicamente planejadas e executadas, seus nomes e imagens já se encontram divulgados em rede mundial. Não há possibilidade alguma de sair ileso dessas situações. As consequências psicológicas para essas vítimas são incalculáveis e, em grande parte das vezes, chegam a atingir seus familiares ou amigos mais próximos.

Além disso, o fato das práticas do cyberbullying serem realizadas, em sua maioria, através de perfis falsos, isentos da identificação real do agressor, torna o problema ainda maior, visto que dificulta buscas e penalidades aos seus praticantes.

Neste sentido, Silva (2015, p. 142) aponta que

> A grande maioria dos praticantes do bullying virtual é composta por adolescentes. No entanto, até o momento, não há uma maneira precisa ou eficaz de traçar o perfil exato desses jovens. Isso ocorre porque os ataques efetuados contra as vítimas são virtuais, e neles a identidade do agressor não se torna pública. Por outro lado, as vítimas, quando descobrem quem são seus bullies virtuais, raramente denunciam. A meu ver, tal postura acoberta e alimenta essa engrenagem covarde e ardilosa que é o cyberbullying.

Silva (2015, p. 142) faz uma abordagem real e, ao mesmo tempo, assustadora, a respeito do cyberbullying e os tempos atuais da modernidade tecnológica ao qual estamos inseridos. Ela diz que

> O cyberbullying é um reflexo perfeito dessa cultura embasada na insensibilidade interpessoal e na total ausência de responsabilidade e solidariedade coletiva. Nesse contexto, o bullying virtual encontra fatores bastante propícios para se proliferar de forma sombriamente imprevisível. Entre eles podemos citar: a inexistência de padrões legais e éticos para a utilização dos recursos tecnológicos de informação e comunicação; a falta de empatia, de sensibilidade e de responsabilidade nas relações interpessoais; a certeza do anonimato, da impunidade dos agressores e do silêncio acuado das vítimas.

Diante deste cenário, considero um grande desafio atuar num segmento tão árido, diante de um quadro constante de agressões virtuais e de graves consequências causadas às vítimas desta prática cruel. Diante dos estudos feitos nesta pesquisa, considero de grande importância a inclusão da segurança digital em ações educativas, orientando e recomendando práticas positivas que, de alguma forma, possam colaborar para uma Internet mais humana, com mais respeito aos direitos humanos digitais.

Mais adiante, ao longo desta pesquisa, serão apresentadas algumas iniciativas que foram identificadas pela pesquisadora, relacionadas à ações de orientação em segurança feitas por organizações não governamentais, empresas (públicas ou privadas), com o intuito de informar a sociedade civil sobre os perigos da Internet e suas inúmeras plataformas digitais, além de promover dicas e recomendações sobre

cuidados no mundo virtual. Estas ações, inclusive, foi parte da construção e consolidação da cartilha “Orientações para uma Internet mais humana”, elaborada pela pesquisadora.

O fato é que há muito o que fazer. Há responsabilidade das famílias, das escolas, dos Governos e da sociedade civil. Como bem afirma Silva (2015, p.178) “Para começar a virar esse jogo, as escolas precisam, inicialmente, reconhecer a existência do bullying e tomar consciência dos prejuízos que ele pode trazer. Bullying é um fato, e não dá mais para botar panos quentes nas evidências”. Além das escolas, entendo ser um problema social, onde há muitas responsabilidades, diante das vidas em jogo. Silva (2015, p. 181) segue neste assunto afirmando que “o bullying é, antes de tudo, uma forma específica de violência. Sendo assim, deve ser identificado, reconhecido e tratado como um problema social complexo e de responsabilidade de todos nós”.

Um pouco do que pode ser feito com as práticas do bullying e cyberbullying será abordado nos parágrafos seguintes.

Neste aspecto, Silva (2015, p. 181) sugere que

> a escola pode e deve representar um papel fundamental na redução desse fenômeno, por meio de programas preventivos e ações combativas nos casos já instalados. Para isso, é necessário que a Instituição escolar atue em parceria com a família dos alunos e com todos os setores da sociedade que lutam pela diminuição da violência em nosso dia a dia. Somente dessa forma seremos capazes de garantir a eficácia de nossos esforços.

A seguir, serão apresentadas algumas iniciativas reais de conteúdos e sites disponibilizados na Internet, construídos e mantidos com o objetivo de incentivar campanhas orientativas para conscientização dos perigos existentes na Internet, explorando dicas e recomendações de segurança.

Estas iniciativas serviram de apoio para construção da cartilha “Orientações para uma Internet mais humana”, elaborada pela pesquisadora, como forma de ser uma ação local na disseminação de cuidados no que diz respeito aos ambientes digitais, incluindo dicas e recomendações em segurança digital.

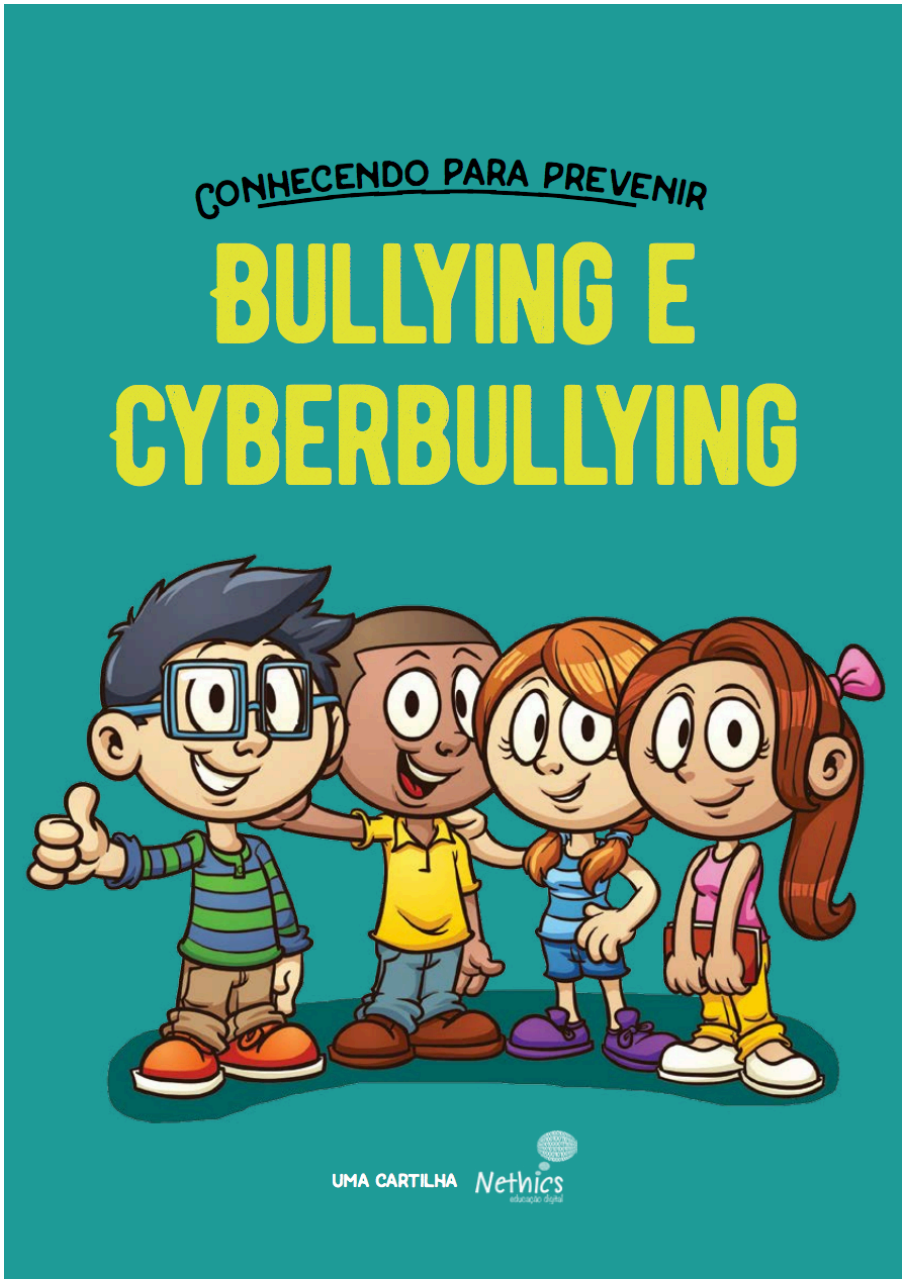
Figura 2. Cartilha da SaferNet Brasil com dicas sobre segurança no uso das redes sociais, chat e webcam para adolescente, jovens, pais e educadores.

Fonte: SAFERNET, 2018.

Além da cartilha apresentada, a SaferNet Brasil, como associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial, possui foco na promoção e defesa dos direitos humanos na Internet do Brasil, os Direitos Humanos Digitais, com inúmeras ações

sociais, realizadas de forma presencial ou através do seu site e inúmeros conteúdos disponíveis.

Figura 3. Cartilha da Nethics Edu de Bullying e Cyberbullying.



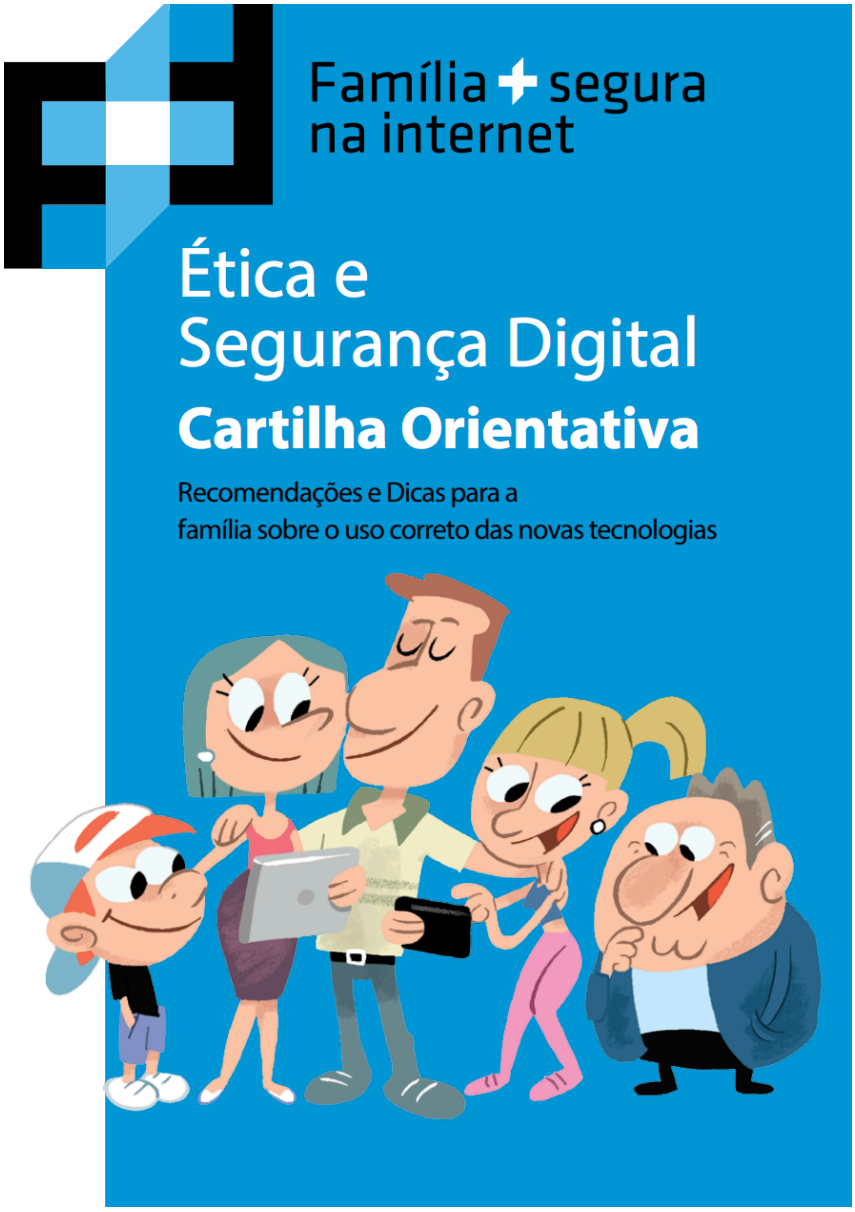
Fonte: NETHICSEDU, 2018.

A “Nethics Educação Digital é uma empresa voltada a educação de crianças, juvenis e adolescentes sobre ou uso ético e seguro da Internet, com o objetivo de firmar e inspirar comportamentos positivos e saudáveis na interação com as tecnologias da informação e comunicação” (Nethics, S/D). É uma Instituição com foco na prevenção

e enfrentamento dos perigos da Internet, sempre orientando e impactando pessoas com conteúdos disponibilizados em seu site na Internet ou através das inúmeras palestras realizadas pelo país. Em seu site, a Nethics (S/D) deixa claro quais são seus propósitos, conforme cita que

> Com criatividade, buscamos despertar o interesse do público infanto-juvenil pela educação digital, transmitindo de forma natural orientações que garantam o melhor e mais seguro proveito da tecnologia. Com informações, orientações, ferramentas e materiais diversificados disponibilizamos subsídios para que os educadores desempenhem seus papeis com excelência neste importante desafio.

Figura 4. Cartilha do Família mais Segura sobre Ética e Segurança Digital.



Fonte: FAMILIAMAISSEGURA, 2018.

O Família mais Segura é mais uma iniciativa de colaborar com a sociedade em prol de uma Internet mais segura. “Movimento para a formação de usuários digitalmente corretos para a construção de um ambiente virtual mais ético, seguro e legal." (Familiamaissegura, 2018).

As ilustrações das cartilhas apresentadas acima são apenas alguns exemplos de conteúdos pesquisados e utilizados, pela pesquisadora, não somente para explorar o universo do bullying e cyberbullying, mas também serviu de apoio para a construção da cartilha “Orientações para uma Internet mais segura”, produto desta pesquisa.

O próximo capítulo vai explorar mais a fundo o cenário dos crimes virtuais. Alguns crimes, inclusive, são praticados através do cyberbullying.

2.4 Crimes Digitais

Entender o conceito e os objetos relacionados aos crimes digitais torna-se importante para promover uma aproximação a respeito do ambiente virtual do cibercrime, os criminosos digitais e alguns tipos de crimes cometidos no ambiente da Internet. Neste sentido,

> “Toda atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital”. (CASSANTI, 2014, p.3)

Os riscos provenientes dos ambientes digitais advêm de hábitos e costumes dos usuários. Inexperiência, inocência, imaturidade ou até mesmo curiosidade são alguns fatores que podem desencadear a prática de um crime digital, em especial, quando as vítimas são crianças e jovens.

Neste contexto, um estudo realizado e publicado um estudo pelo Center for Cyber Safety and Education, nos Estados Unidos, fruto de uma parceria entre o (ISC)²® e com a empresa de consultoria Booz Allen Hamilton, sobre o comportamento on-line

de crianças, faz uma análise comparada, com base no autorrelato de adolescentes entre as 4ª e 8ª séries com a declaração dos pais quanto às condutas observadas.

Como fundação sem fins lucrativos do (ISC)², o Center for Cyber Safety and Education é autoridade mundial em educação em segurança na Internet, que oferece, desde 2011, o programa Safe and Secure Online®. O projeto gratuito pioneiro ensina crianças, pais, professores e idosos ao redor do mundo sobre como manter a segurança on-line. (Decision Report, JUN 2016)

Alguns dados importantes obtidos pela pesquisa:

A) *40% das crianças pesquisadas disseram que se conectam ou conversam on-line com estranhos.*
B) *21% levaram o relacionamento adiante e conversaram com um desconhecido ao telefone.*
C) *15% tentaram se encontrar com o primeiro estranho que elas conheceram on-line.*
D) *11% se encontraram com um desconhecido em sua casa, na casa do estranho, em parques, shoppings ou restaurantes – muitas vezes acompanhadas por um amigo.*
E) *30% relataram mandar mensagens de seus telefones para um estranho.*
F) *25% passaram seus números de telefone para um desconhecido.*
G) *6% revelaram seus endereços.*
H) *53% das crianças que participaram da pesquisa acessam a Internet a semana toda por razões que não têm relação com lições de casa.*
I) *49% permaneceram on-line depois das 23h ou mais tarde em dias de aulas.*

Quais os motivadores que levam crianças a conversar online com estranhos? Que efeitos estas ações podem provocar? Conversar com estranhos, independente do assunto, pode criar uma proximidade com alguém que não se conhece, não se sabe sua idade, hábitos, escolhas, principalmente ao considerar que a conversa é entre uma criança e um estranho, o risco é bem maior.

O que leva um jovem a comunicar com um estranho periodicamente? O risco aumenta, à medida que se estreita o relacionamento. A partir daí muitas informações sobre sua vida pessoal podem ser facilmente conseguidas, a partir de uma conversa informal, adequada à idade da criança, utilizando, inclusive, técnicas de “Engenharia Social” que, no contexto de segurança da informação, refere-se a manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais. Ela faz com que pessoas façam coisas que normalmente não fariam para um estranho.

Nesta mesma temática, Mitnick & Simon (2003, xiii) afirmaram que “O engenheiro social é alguém que usa a fraude, a influência e a persuasão”. Já Cassanti (2014, p. 15) refere-se ao engenheiro social como alguém que “utilizará algumas técnicas de persuasão, estimulando o MEDO, a CURIOSIDADE, a GANÂNCIA ou a SIMPATIA da vítima para obter a informação ou acesso desejado”.

Nas duas citações, observa-se o uso de características pessoais para promover ataques a vítimas, muito mais do que simplesmente o uso de tecnologias para obtenção de alguma informação valiosa ou para cometimento de algum crime na vida real.

É importante incorporar conteúdos e novos saberes sobre riscos e cuidados com uso da Internet, além de dicas sobre comportamento seguro na Internet, principalmente para indivíduos ainda em formação, não preocupados com a exposição de sua vida nas redes sociais. São conhecidos como nativos digitais.

Em “Educ@ar, a revolução digital na educação” (2013), Martha Gabriel apresenta conceitos importantes que facilita o entendimento a respeito de gerações.

> No mundo ocidental, as principais classificações recentes de gerações nos últimos 50 anos, são:
>
> - Baby Boomers (nascidos de 1946 a 1964) – é a geração que nasceu após a Segunda Guerra Mundial, que foi marcada por um aumento das taxas de natalidade.
>
> - Geração X (nascidos entre 1960 e início dos anos 1980).

> - Geração Y (nascidos entre 1980 e início da década de 2000) – também conhecida como *Millenials, Generation Next e Echo Boomers*.
>
> - Geração Z (nascidos a partir do início da década de 2000) – também conhecida como iGeneration, Generation@, Net Generation, Generation AO (Always On), Generation Text e **Nativos Digitais.**
>
> (GABRIEL, 2013, p. 86)

A “Geração Z” ou também conhecida como os “Nativos Digitais” já nasceram em um mundo repleto de tecnologias, um mundo eminentemente interconectado, hiperconectado, onde o acesso a qualquer informação é feito em segundos, onde expor informações depende de poucos “cliques”, onde falar e comunicar-se, com desconhecidos inclusive, não é algo difícil de realizar.

Crianças e adolescentes tornam-se alvos fáceis de pessoas mal intencionadas, engenheiros sociais ou criminosos digitais em busca de informações privilegiadas, visando um objetivo fim. Informações sobre a vida pessoal, familiar, escolar e social, até hábitos pessoais transformam-se em informações valiosas para o crime digital, seja para a venda indevida de dados pessoais em mercados paralelos como a “Deep Web”, seja para planejar e cometer crimes na vida real, a partir de dados que os indivíduos expõem sobre suas vidas nas redes sociais.

Martha Gabriel (2018, p. 61), em seu livro “Você, eu e os robôs”, faz uma observação esclarecedora a respeito dos cuidados necessários que todos devem ter sobre sua vida digital, da mesma forma que nos ambientes digitais da Internet. Ela cita que

> “É necessário que tomemos consciência de que cada ação que praticamos nos ambientes digitais pode ter consequências tanto positivas como negativas, e, dessa forma, precisamos pensar com critério sobre o que deve ou não ser publicado em cada ambiente”. (GABRIEL, 2018, p. 61).

Ambientes digitais são espaços de disseminação excessiva de todo tipo de informações pessoais.

> “Da mesma forma que pensamos sobre o que devemos ou não falar em cada lugar off-line físico em que estamos presentes – em casa com a família, no clube com amigos, na escola, na igreja, no trabalho, etc – devemos fazer o mesmo nos ambientes digitais, que são o habitat natural da proliferação digital de dados de todos os tipos, inclusive informações pessoais” (GABRIEL, 2018, p. 61).

É mister a disseminação de ações educativas de segurança digital com o objetivo de prestar esclarecimentos sobre as possíveis consequências geradas pelo excesso de exposição, ou por acessar ambientes digitais de reputação não ilibada, ou por acessar e se envolver com grupos que espalham ódio e violência digital na Internet, e tantos outros motivos. Os crimes são virtuais, mas as vítimas são reais.

Segundo o Ministério Público da Paraíba,

> Muitos agressores (cyberbullying) já foram identificados e responderam a processos, seja na área civil (danos morais) ou infração (medida socioeducativa – adolescente, ou sanção penal – a partir dos 18 anos de idade). Na web, os agressores virtuais, sejam adolescentes ou adultos, sempre deixam rastros, o que facilita a identificação, o trabalho de investigação e a consequente responsabilização. Delegacias especializadas em Crimes Cibernéticos já dispõem de recursos para identificar a origem mensagens virtuais. (PARAÍBA, 2009, p. 14)

A relação do cyberbullying com os crimes digitais é tênue. A respeito deste assunto, Silva (2015, p. 136) cita que

> Os sites de relacionamentos, as comunidades e os blogs há muito tempo são usados para promover ataques vexatórios com o intuito sórdido de excluir ou humilhar os agredidos. Comentários racistas, preconceituosos e sexistas são feitos de forma totalmente desrespeitosa e, muitas vezes, vêm acompanhados de fotografias alteradas das vítimas em montagens constrangedoras e bizarras.

Observa-se que o cyberbullying pode gerar crimes digitais, a depender do tipo de prática cometida, o que será abordado mais adiante.

O número de crimes cometidos através dos meios digitais é bem extenso. Serão apresentados, a seguir, alguns indicadores de crimes digitais, divulgados pela Safernet[3] que desde 2005, a Safernet atua como disseminador dos índices relacionados aos crimes digitais, além de contribuir, substancialmente, com conteúdos educativos e de conscientização em segurança digital. Ela é considerada uma referência nacional no combate e enfrentamento aos crimes e violações de Direitos

[3] Uma associação civil de direito privado, com atuação nacional, sem fins lucrativos ou econômicos, sem vinculação político partidária, religiosa ou racial. Fundada em 20 de dezembro de 2005, com foco na promoção e defesa dos Direitos Humanos na Internet no Brasil. (SAFERNET, S/D).

Humanos na Internet, além de possuir acordos de cooperação importantes com Órgãos Governamentais, a exemplo do Ministério Público Federal.

> Naquela época, era urgente a necessidade de oferecer uma resposta eficiente, consistente e permanente no Brasil para os graves problemas relacionados ao uso indevido da Internet para a prática de crimes e violações contra os Direitos Humanos. Aliciamento, produção e difusão em larga escala de imagens de abuso sexual de crianças e adolescentes, racismo, neonazismo, intolerância religiosa, homofobia, apologia e incitação a crimes contra a vida já eram crimes cibernéticos atentatórios aos Direitos Humanos presentes na rede". (SAFERNET, S/D)

"Nosso ideal é transformar a Internet em um ambiente ético e responsável, que permita às crianças, jovens e adultos criarem, desenvolverem e ampliarem relações sociais, conhecimentos e exercerem a plena cidadania com segurança e liberdade". (SAFERNET, S/D)

Vejamos o caso da "**Pedofilia**" e "**Pornografia Infantil**".

Pedofilia consiste em

> produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da web, e-mail, newsgroups, salas de bate-papo (chat), ou qualquer outra forma. Compreende, ainda, o uso da Internet com a finalidade de aliciar crianças ou adolescentes para realizarem atividades sexuais ou para se exporem de forma pornográfica. (CASSANTI, 2014, p. 30)

Associar alguma motivação psicológica de uma pessoa mal intencionada com exposição excessiva de informações postadas por crianças e adolescentes na Internet pode ser uma fórmula explosiva que culmine num crime real de pedofilia.

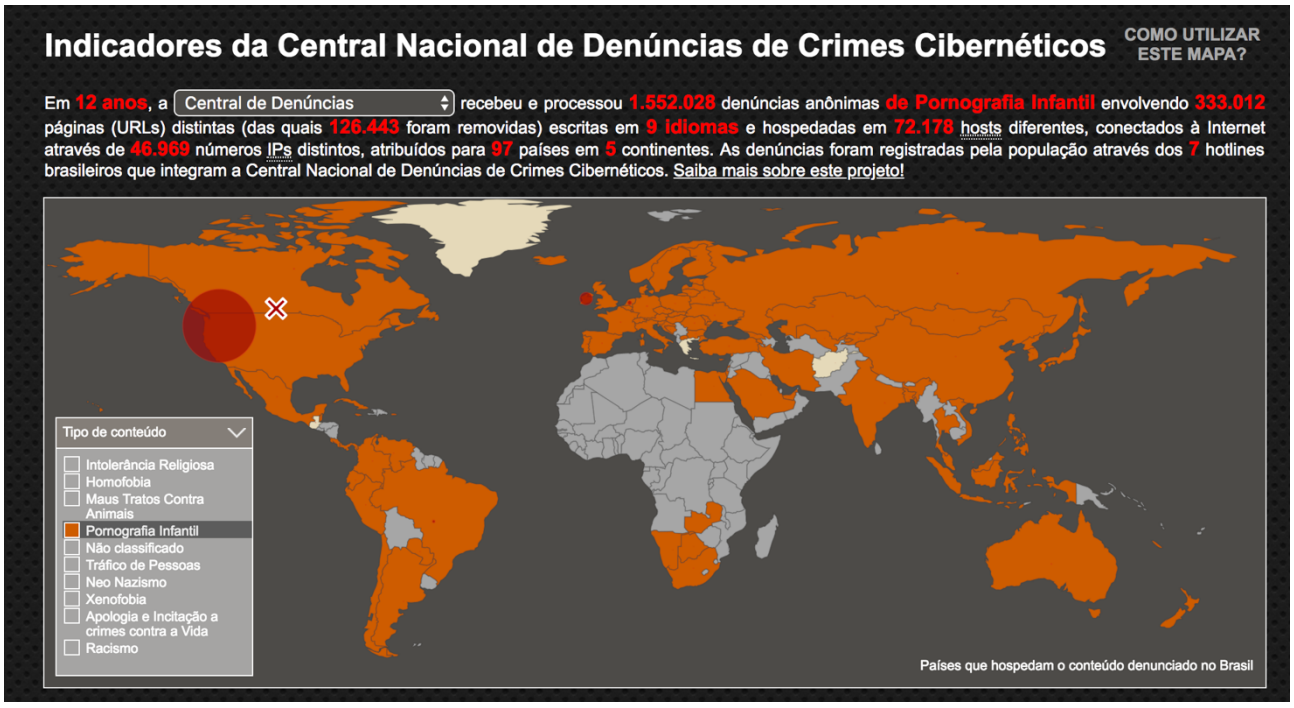
> Para conquistar a confiança das crianças e dos adolescentes os criminosos utilizam perfis falsos e uma linguagem diferenciada, com intuito de programar encontros virtuais e presenciais que viabilizam a prática de atos de violência sexual. Em muitos casos oferecem oportunidades imperdíveis, presentes ou até mesmo dinheiro para convencer a vítima a marcar um encontro ou pedem para que se façam fotos e vídeos pornográficos. (CASSANTI, 2014, p. 30)

É estarrecedora a quantidade de informações adquiridas em fonte aberta, ou seja, divulgada abertamente na Internet, sendo possível para os agressores acompanhar suas vítimas, estudá-las, verificar seus hábitos e ver a melhor forma de ataque.

A seguir, são apresentados alguns gráficos com indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, contendo informações coletadas através do canal do canal “Hotline” da Safernet, que é um serviço oferecido visando o recebimento de denúncias anônimas de crimes e violações contra os Direitos Humanos na Internet. Estes gráficos tratam de crimes relativos à pornografia infantil, realizados através da Internet, com dados da Central de Denúncias, da Polícia Federal, da Secretaria de Direitos Humanos e da própria Safernet.

Este canal “Hotline” da Safernet conta com suporte de Órgãos Governamentais e parcerias com empresas privadas, autoridades policiais e judiciais para dar seguimento a ações que visem o combate ao crime, culminando, em muitos casos, na prisão de agressores e criminosos.

Figura 5. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Pornografia Infantil. Dados da Central de Denúncias.

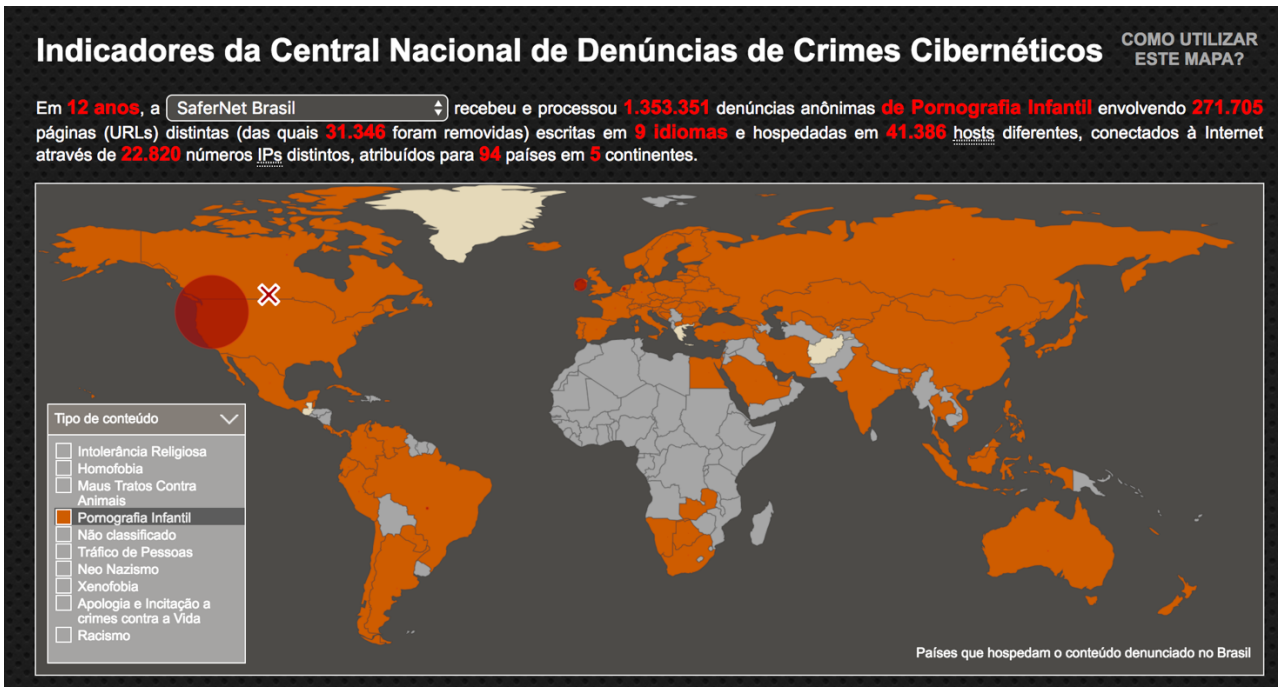


Fonte: SAFERNET, 2018.

Neste gráfico, a Central de Denúncias recebeu, em 12 anos, 1.552.028 denúncias anônimas de pornografia infantil, envolvendo mais de 300 mil páginas da Internet hospedadas em mais de 90 países dos 5 continentes. As denúncias foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Os dados são estarrecedores, considerando que estes são apenas os registrados através de denúncias anônimas. O número, portanto, é maior, porém não há informações a cerca do número real de casos.

Figura 6. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Pornografia Infantil. Dados da Safernet Brasil.

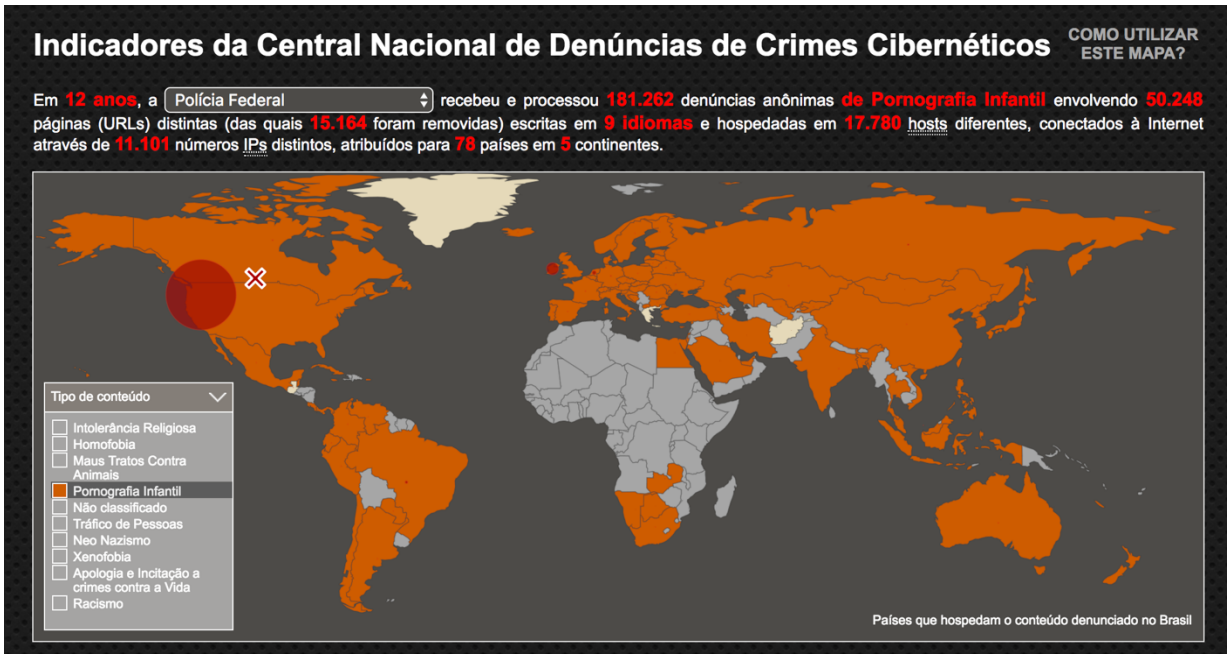


Fonte: SAFERNET, 2018.

Somando-se aos dados do gráfico anterior, o mesmo tipo de denúncia de casos relativos à pornografia infantil, a Safernet recebeu, em 12 anos, 1.353.351 denúncias anônimas de pornografia infantil, envolvendo quase 300 mil páginas da Internet hospedadas em mais de 90 países dos 5 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Dados igualmente estarrecedores que os dados anteriores. Somando-se os dados dos dois gráficos, chegamos ao subtotal de 2.905.379 de denúncias anônimas de pornografia infantil, ao longo de 12 anos de atuação. A este subtotal ainda serão acrescentados dados dos próximos dois gráficos, referentes à denúncias de outros Órgãos parceiros da Central de Denúncias.

Figura 7. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Pornografia Infantil. Dados da Polícia Federal.



Fonte: SAFERNET, 2018.

Somando-se aos dados dos dois gráficos anteriores, o mesmo tipo de denúncia de casos relativos à pornografia infantil. Neste gráfico, a Polícia Federal recebeu, em 12 anos, 181.262 denúncias anônimas de pornografia infantil, envolvendo pouco mais de 50 mil páginas da Internet hospedadas em mais de 70 países dos 5 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Somando-se estes dados aos dois gráficos anteriores, chegamos ao novo subtotal de 3.086.641 de denúncias anônimas de pornografia infantil, ao longo de 12 anos de atuação. A este subtotal também serão acrescentados dados referentes à denúncias de mais um Órgão parceiro da Central de Denúncias.

Figura 8. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Pornografia Infantil. Dados da Secretaria de Direitos Humanos.

Fonte: SAFERNET, 2018.

Somando-se aos dados do gráfico anterior, o mesmo tipo de denúncia de casos relativos à pornografia infantil. Neste gráfico, a Secretaria de Direitos Humanos recebeu, em 12 anos, 8.822 denúncias anônimas de pornografia infantil, envolvendo quase 3 mil páginas da Internet hospedadas em 39 países dos 5 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Dados igualmente estarrecedores que os dados anteriores. Somando-se os dados dos dois gráficos, chegamos ao total geral de 3.095.463 de denúncias anônimas de pornografia infantil, ao longo de 12 anos de atuação das quatro instituições parceiras e integrantes da Central de Denúncias de Crimes Cibernéticos.

Silva (2015, p. 141) cita que “as vítimas de cyberbullying podem ainda atrair pessoas inescrupulosas que, no mundo real, utilizam as imagens expostas na rede mundial como mercadoria que alimenta a indústria de pornografia e pedofilia”. Observa-se aqui a estreita relação entre a prática do cyberbullying e crimes como a pedofilia infantil,

tratando-se como crime digital, considerando que foi feito uso das tecnologias para tal ato.

Faço algumas análises e conclusões importantes, feitas a partir das informações registradas nos gráficos dos indicadores:

A) 173.484 páginas foram removidas, após denúncias registradas e medidas cabíveis realizadas para promover a retirada de conteúdos criminosos relacionados à pornografia infantil exposta na Internet. Este número representa 26,37% do total de páginas envolvidas com as denúncias (657.872). O percentual é muito baixo, menos de 30% de páginas removidas após denúncia e processo judicial, considerando um número elevado de páginas denunciadas que representam mais de meio milhão.

B) As páginas denunciadas estavam hospedadas em diversos países dos 5 continentes, ou seja, trata-se de um problema global, não somente local, considerando a possibilidade e viabilidade técnica de registro de páginas web (URLs) em países distintos.

   Em alguns casos, o pedido de retirada de um site (URL) do ar acaba demorando, em função de processos jurídicos que acompanham os encaminhamentos das denúncias. Isso significa que, uma página pode permanecer ativa, “no ar”, durante muito tempo, até que um processo se conclua e sejam solicitadas as providências cabíveis aos responsáveis pelos endereços de Internet (domínios) em cada país.

C) As páginas envolvidas nas denúncias realizadas estavam hospedadas em 178.163 hosts (máquinas hospedeiras que armazenam sites), não estando claro se o host de uma denúncia é o mesmo de uma outra denúncia.

D) Em todas as denúncias, é informado que as páginas foram escritas em 9 idiomas, mas não cita nem especifica quais idiomas.

E) Os maiores índices de denúncias são feitos na seguinte ordem descrescente: Safernet Brasil, Central de Denúncias, Polícia Federal e Secretaria de Direitos Humanos. As diferenças nos números de denúncias são bem grandes entre os 2 primeiros órgãos e os 2 últimos, porém, não está claro o motivo desta diferença. Há possibilidade de uma correlação com ações de divulgação dos canais de denúncia, visibilidade do órgão na Internet, divulgação de ações educativas, porém, isto são inferências, não há evidências sobre o assunto.

Vejamos o caso do "**Racismo**".

A Declaração Universal de Direitos Humanos (DUDH), em seu artigo 2o, cita que "Todos os seres humanos podem invocar os direitos e as liberdades proclamados na presente Declaração, sem distinção alguma, nomeadamente de raça, de cor, de sexo, de língua, de religião, de opinião política ou outra, de origem nacional ou social, de fortuna, de nascimento ou de qualquer outra situação." (Nações Unidas).

Infelizmente, apesar de todos os serem humanos serem notadamente iguais, perante a própria DUDH, observam-se, diariamente, casos de abusos de direitos humanos com casos diversos de racismo, inclusive cometidos através dos espaços digitais da Internet.

Racismo é caracterizado como "Material escrito, imagens ou qualquer outro tipo de representação de idéias ou teorias que promovam e/ou incitem o ódio, a discriminação ou violência contra qualquer indivíduo ou grupo de indivíduos, baseado na raça, cor, religião, descendência ou origem étnica ou nacional." (Safernet)

A seguir, é apresentado um gráfico com indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, contendo informações coletadas através do canal do canal "Hotline" da Safernet, com crimes relativos ao racismo, realizados através da Internet.

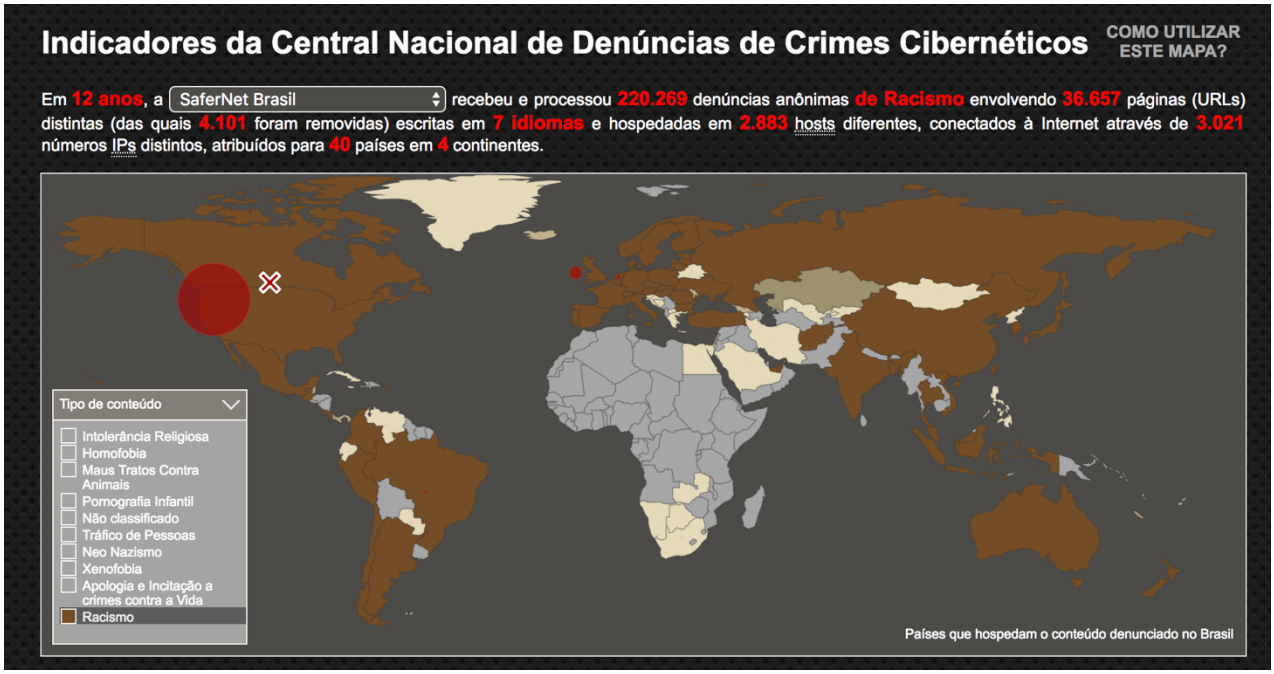
Figura 9. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas ao Racismo. Dados da Central de Denúncias.

Fonte: SAFERNET, 2018.

Neste gráfico, a Central de Denúncias recebeu, em 12 anos, 3.925.405 denúncias anônimas de racismo, envolvendo mais de 700 mil páginas da Internet hospedadas em mais de 100 países dos 5 continentes. As denúncias foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Os dados são maiores que os dados relativos às denúncias feitas de pornografia infantil e, do mesmo modo, são apenas os casos registrados através de denúncias anônimas, concluindo-se que número é maior, porém não há informações a cerca do número real de casos.

Figura 10. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas ao Racismo. Dados da Safernet Brasil.



Fonte: SAFERNET, 2018.

Somando-se aos dados do gráfico anterior, o mesmo tipo de denúncia de casos relativos à pornografia infantil, a Safernet Brasil recebeu, em 12 anos, 220.269 denúncias anônimas de racismo, envolvendo quase 40 mil páginas da Internet hospedadas em 40 países de 4 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Somando-se os dados dos dois gráficos, chegamos ao subtotal de 4.145.674 de denúncias anônimas relativas ao racismo, ao longo de 12 anos de atuação da central de denúncias. A este subtotal ainda serão acrescentados dados dos próximos dois gráficos, referentes à denúncias de outros Órgãos parceiros da Central de Denúncias.

Figura 11. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Racismo. Dados da Polícia Federal.

Fonte: SAFERNET, 2018.

Neste gráfico, a Polícia Federal recebeu, em 12 anos, 332.297 denúncias anônimas de racismo, envolvendo pouco mais de 50 mil páginas da Internet hospedadas em quase 60 países dos 5 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Somando-se estes dados aos dois gráficos anteriores, chegamos ao novo subtotal de 4.477.971 de denúncias anônimas de racismo, ao longo de 12 anos de atuação. A este subtotal também serão acrescentados dados referentes à denúncias de mais um Órgão parceiro da Central de Denúncias.

Figura 12. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas ao Racismo. Dados da Secretaria de Direitos Humanos.

Fonte: SAFERNET, 2018.

Somando-se aos dados do gráfico anterior, o mesmo tipo de denúncia de casos relativos ao racismo. Neste gráfico, a Secretaria de Direitos Humanos recebeu, em 12 anos, 10.137 denúncias anônimas de racismo, envolvendo mais de 3 mil páginas da Internet hospedadas em 19 países de 4 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Somando-se os dados dos dois gráficos, chegamos ao total geral de 4.488.108 de denúncias anônimas de racismo, ao longo de 12 anos de atuação das quatro instituições parceiras e integrantes da Central de Denúncias de Crimes Cibernéticos.

Faço algumas análises e conclusões importantes, feitas a partir das informações registradas nos gráficos dos indicadores:

A) 48.305 páginas foram removidas, após denúncias registradas e medidas cabíveis realizadas para promover a retirada de conteúdos criminosos relacionados ao racismo, expostos na Internet. Este número representa 6,09% do total de páginas envolvidas com as denúncias (792.722). O percentual é

extremamente baixo, apenas 6% de páginas removidas após denúncia e processo judicial, considerando um número elevado de páginas denunciadas que representam mais de 700 mil.

B) As páginas denunciadas estavam hospedadas em diversos países dos 5 continentes, em alguns casos foram denúncias de países de 4 continentes (Safernet e Secretaria de Direitos Humanos). Trata-se de um problema global, não somente local, considerando a possibilidade e viabilidade técnica de registro de páginas web (URLs) em países distintos.

   Em alguns casos, o pedido de retirada de um site (URL) do ar acaba demorando, em função de processos jurídicos que acompanham os encaminhamentos das denúncias. Isso significa que, uma página pode permanecer ativa, “no ar”, durante muito tempo, até que um processo se conclua e sejam solicitadas as providências cabíveis aos responsáveis pelos endereços de Internet (domínios) em cada país.

C) As páginas envolvidas nas denúncias realizadas estavam hospedadas em 102.856 hosts (máquinas hospedeiras que armazenam sites), não estando claro se o host de uma denúncia é o mesmo de uma outra denúncia.

D) Nas denúncias, é informado que as páginas foram escritas em 5, 7 e 9 idiomas, dependendo do canal de denúncia que recebeu o registro, mas não cita nem especifica quais idiomas.

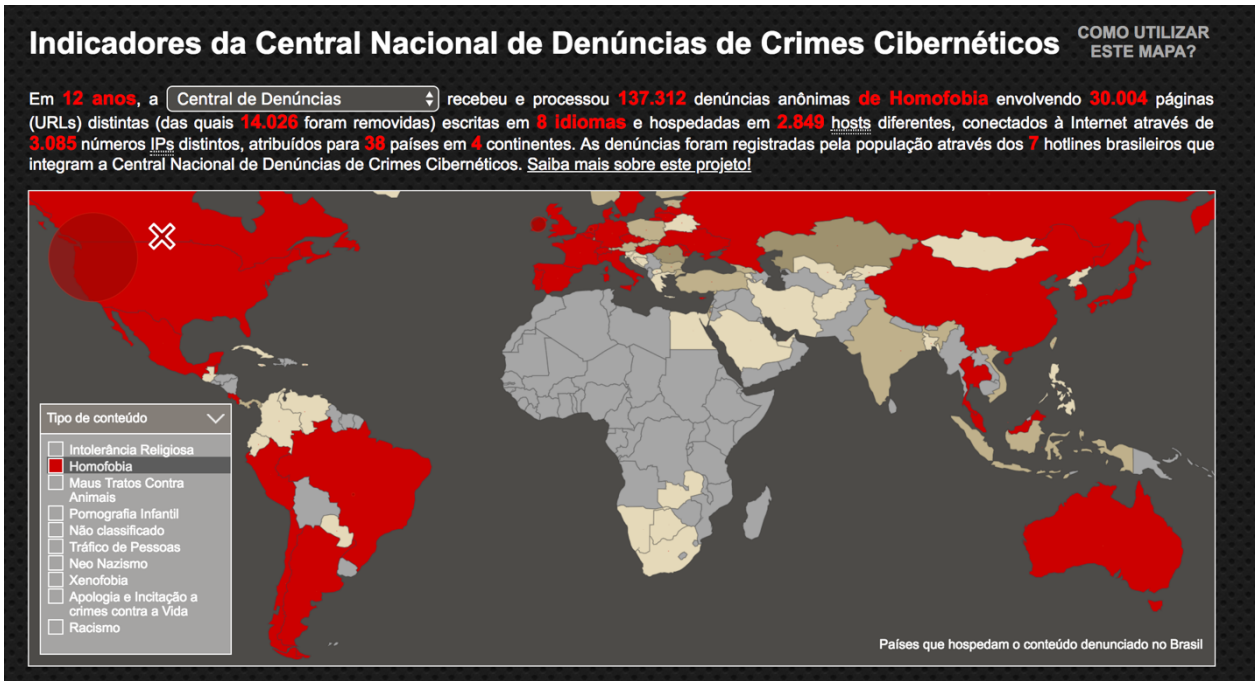
E) Os maiores índices de denúncias são feitos na seguinte ordem descrescente: Central de Denúncias, Polícia Federal, Safernet Brasil e Secretaria de Direitos Humanos. As diferenças nos números de denúncias são maiores entre os 3 primeiros órgãos em detrimento do último órgão de recebimento de denúncia, porém, não está claro o motivo desta diferença. Há possibilidade de uma correlação com ações de divulgação dos canais de denúncia, visibilidade do órgão na Internet, divulgação de ações educativas, porém, isto são inferências, não há evidências sobre o assunto.

Vejamos o caso da “**Homofobia**”.

“As leis penais em vigor no Brasil ainda não prevêem o crime de homofobia, em que pese a Constituição Federal de 1988 determinar que Constituem objetivos fundamentais da República Federativa do Brasil: promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação - Art. 3º, XLI e ainda que a lei punirá qualquer discriminação atentatória dos direitos e liberdades fundamentais - Art. 5º, XLI. Sendo assim, de acordo com o mandamento constitucional e entendendo ser esta prática atentatória aos Direitos Humanos e lesiva ao interesse da sociedade, a SaferNet Brasil rastreará as denúncias recebidas e as encaminhará para as instituições pertinentes.” (Safernet).

A seguir, é apresentado um gráfico com indicadores da Central Nacional de Denúncias de Crimes Cibernéticos, contendo informações coletadas através do canal do canal “Hotline” da Safernet, com crimes relativos à homofobia, realizados através da Internet.

Figura 13. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Homofobia. Dados da Central de Denúncias.

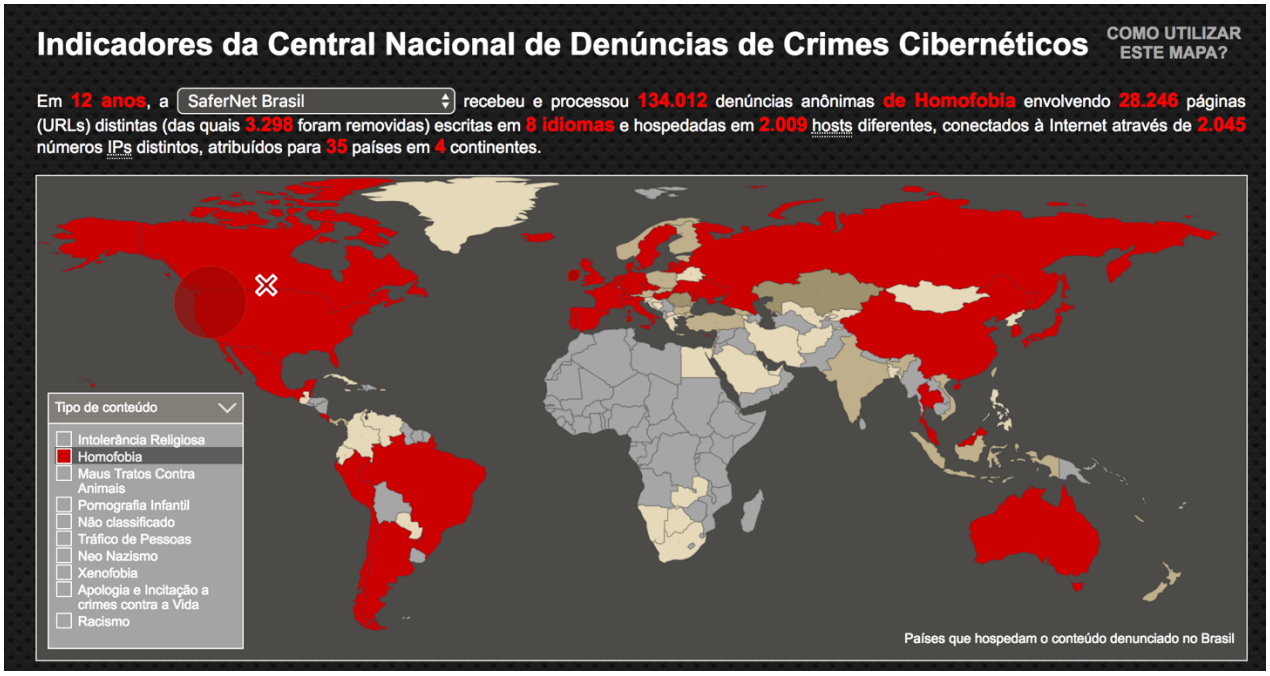


Fonte: SAFERNET, 2018.

Neste gráfico, a Central de Denúncias recebeu, em 12 anos, 137.213 denúncias anônimas de homofobia, envolvendo mais de 30 mil páginas da Internet hospedadas em mais de 30 países dos 4 continentes. As denúncias foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Os dados são maiores que os dados relativos às denúncias feitas de homofobia e, do mesmo modo, são apenas os casos registrados através de denúncias anônimas, concluindo-se que número é maior, porém não há informações a cerca do número real de casos.

Figura 14. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Homofobia. Dados da Safernet Brasil.



Fonte: SAFERNET, 2018.

Somando-se aos dados do gráfico anterior, o mesmo tipo de denúncia de casos relativos à homofobia, a Safernet Brasil recebeu, em 12 anos, 134.012 denúncias anônimas de racismo, envolvendo quase 30 mil páginas da Internet hospedadas em 35 países de 4 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

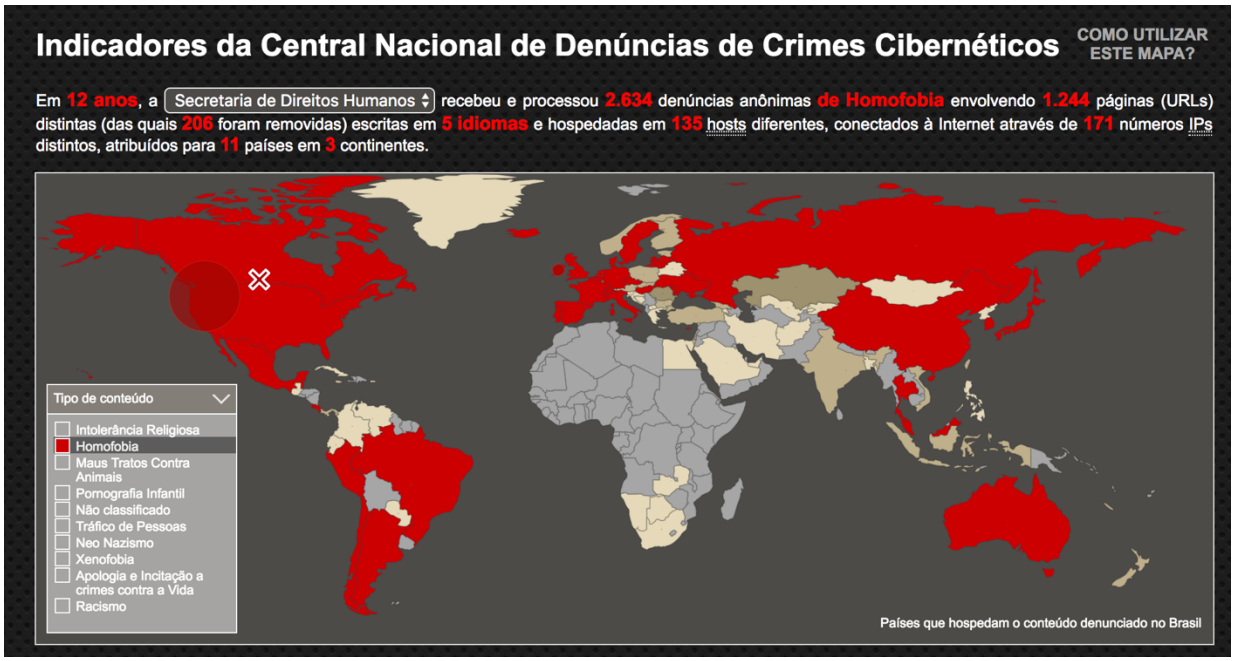
Somando-se os dados dos dois gráficos, chegamos ao subtotal de 271.324 de denúncias anônimas relativas à homofobia, ao longo de 12 anos de atuação da central de denúncias. A este subtotal ainda serão acrescentados dados dos próximos dois gráficos, referentes a denúncias de outros Órgãos parceiros da Central de Denúncias.

Figura 15. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Homofobia. Dados da Polícia Federal.

Fonte: SAFERNET, 2018.

Conforme apresenta o gráfico acima, não foram encontrados registros de denúncias feitas à Polícia Federal de casos relativos à homofobia. Fazendo uma inferência, é possível ter havido erro no contador de denúncias da página apresentada ou em algum contador. Mas isso não é conclusivo.

Figura 16. Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos. Números de denúncias anônimas registradas, relativas à Homofobia. Dados da Secretaria de Direitos Humanos.



Fonte: SAFERNET, 2018.

Neste gráfico, a Secretaria de Direitos Humanos recebeu, em 12 anos, 2.634 denúncias anônimas de racismo, envolvendo pouco mais de mil páginas da Internet hospedadas em 11 países de 3 continentes. As denúncias também foram feitas por pessoas através dos canais de atendimento e denúncia no Brasil que integram a Central de Denúncias de Crimes Cibernéticos.

Somando-se os dados dos dois gráficos, chegamos ao total geral de 273.958 de denúncias anônimas de homofobia, ao longo de 12 anos de atuação das quatro instituições parceiras e integrantes da Central de Denúncias de Crimes Cibernéticos.

Faço algumas análises e conclusões importantes, feitas a partir das informações registradas nos gráficos dos indicadores:

A) 17.530 páginas foram removidas, após denúncias registradas e medidas cabíveis realizadas para promover a retirada de conteúdos criminosos relacionados à homofobia, expostos na Internet. Este número representa 29,46% do total de páginas envolvidas com as denúncias (59.494). O percentual de páginas retiradas é mais alto que os indicadores relativos à pornografia infantil e racismo.

B) As páginas denunciadas estavam hospedadas em diversos países dos 4 continentes, em alguns casos foram denúncias de países de 3 continentes. Trata-se de um problema global, não somente local, considerando a possibilidade e viabilidade técnica de registro de páginas web (URLs) em países distintos.

   Em alguns casos, o pedido de retirada de um site (URL) do ar acaba demorando, em função de processos jurídicos que acompanham os encaminhamentos das denúncias. Isso significa que, uma página pode permanecer ativa, “no ar”, durante muito tempo, até que um processo se conclua e sejam solicitadas as providências cabíveis aos responsáveis pelos endereços de Internet (domínios) em cada país.

C) As páginas envolvidas nas denúncias realizadas estavam hospedadas em 4.993 hosts (máquinas hospedeiras que armazenam sites), não estando claro se o host de uma denúncia é o mesmo de uma outra denúncia.

D) Nas denúncias, é informado que as páginas foram escritas em 5 e 8 idiomas, dependendo do canal de denúncia que recebeu o registro, mas não cita nem especifica quais idiomas.

E) Os maiores índices de denúncias são feitos na seguinte ordem decrescente: Central de Denúncias, Safernet Brasil e Secretaria de Direitos Humanos. Não houve informações da Polícia Federal. As diferenças nos números de

denúncias são maiores entre os 2 primeiros órgãos em detrimento do último órgão de recebimento de denúncia, porém, não está claro o motivo desta diferença. Há possibilidade de uma correlação com ações de divulgação dos canais de denúncia, visibilidade do órgão na Internet, divulgação de ações educativas, porém, isto são inferências, não há evidências sobre o assunto.

A seguir, é feita uma consolidação de todos os dados analisados e apresentados, referentes às denúncias feitas aos órgãos componentes da Central de Denúncias de Crimes Cibernéticos, relativos aos indicadores de pornografia infantil, racismo e homofobia.

Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Pornografia Infantil.

Figura 17. Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Pornografia Infantil.

PORNOGRAFIA INFANTIL					
ÓRGÃO	TOTAL DE DENÚNCIAS	TOTAL DE PÁGINAS	PÁGINAS REMOVIDAS	HOSTS	PAÍSES
CENTRAL DE DENÚNCIAS	1.552.028	333.012	126.443	72.178	97
SAFERNET BRASIL	1.353.351	271.705	31.346	41.386	94
POLÍCIA FEDERAL	181.262	50.248	15.164	17.780	78
SECRETARIA DE DIREITOS HUMANOS	8.822	2.907	531	1.160	39
TOTAL GERAL	**3.095.463**	**657.872**	**173.484**	**132.504**	**308**

Fonte: Elaborado pela autora através de dados da SAFERNET, 2018.

Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos ao Racismo.

Figura 18. Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos ao Racismo.

RACISMO					
ÓRGÃO	TOTAL DE DENÚNCIAS	TOTAL DE PÁGINAS	PÁGINAS REMOVIDAS	HOSTS	PAÍSES
CENTRAL DE DENÚNCIAS	567.497	96.179	32.095	11.306	62
SAFERNET BRASIL	220.269	36.657	4.101	2.883	40
POLÍCIA FEDERAL	332.297	51.529	11.435	5.477	59
SECRETARIA DE DIREITOS HUMANOS	10.137	3.312	674	341	19
TOTAL GERAL	1.130.200	187.677	48.305	20.007	180

Fonte: Elaborado pela autora através de dados da SAFERNET, 2018.

Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Homofobia.

Figura 19. Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Homofobia.

HOMOFOBIA					
ÓRGÃO	TOTAL DE DENÚNCIAS	TOTAL DE PÁGINAS	PÁGINAS REMOVIDAS	HOSTS	PAÍSES
CENTRAL DE DENÚNCIAS	137.312	30.004	14.026	2.849	38
SAFERNET BRASIL	134.012	28.246	3.298	2.009	35
POLÍCIA FEDERAL	0	0	0	0	0
SECRETARIA DE DIREITOS HUMANOS	2.634	1.244	206	135	11
TOTAL GERAL	273.958	59.494	17.530	4.993	84

Fonte: Elaborado pela autora através de dados da SAFERNET, 2018.

Totais Gerais dos Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Pornografia Infantil, Racismo e Homofobia.

Figura 20. Totais Gerais dos Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos aos 3 crimes cibernéticos objetos da análise.

TOTAIS GERAIS					
CRIME CIBERNÉTICO	TOTAL DE DENÚNCIAS	TOTAL DE PÁGINAS	PÁGINAS REMOVIDAS	HOSTS	PAÍSES
PORNOGRAFIA INFANTIL	3.095.463	657.872	173.484	132.504	308
RACISMO	1.130.200	187.677	48.305	20.007	180
HOMOFOBIA	273.958	59.494	17.530	4.993	84
TOTAL GERAL	4.499.621	905.043	239.319	157.504	572

Fonte: Elaborado pela autora através de dados da SAFERNET, 2018.

Pode-se observar, a partir dos dados apresentados, que pornografia infantil é o campeão de denúncias feitas na Central Nacional de Denúncias de Crimes Cibernéticos. Apesar de homofobia ter sofrido impacto nos números, em função da ausência de dados provenientes do canal de denúncia da Polícia Federal, os números de casos de homofobia registrados estão bem abaixo que os outros dois indicadores, pornografia infantil e racismo.

Este dado é um indicador que demonstra a importância e necessidade de promover estudos mais profundos, visando o entendimento dos conteúdos de cada indicador, além de buscar e propor ações que sirvam de instrumentos para o combate dos crimes cibernéticos.

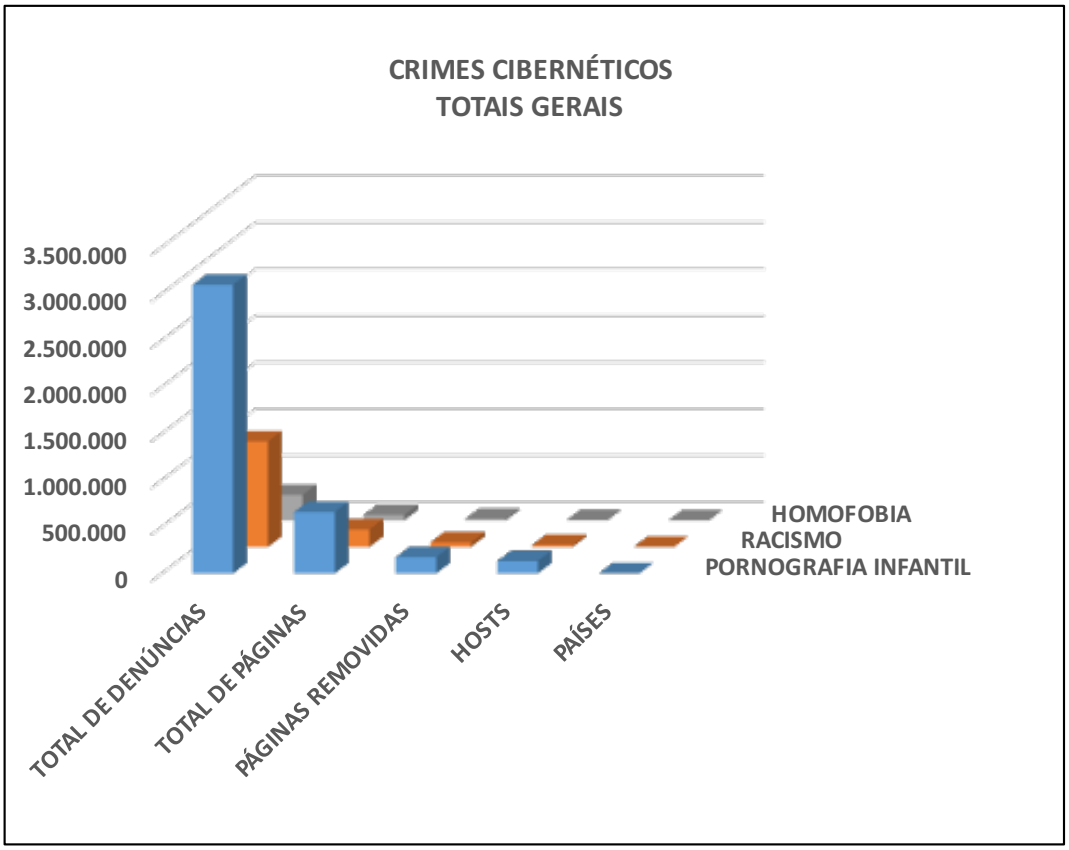
A autora conclui que, com base nos dados mapeados, analisados e apresentados, ações educativas em segurança digital são necessárias para que indivíduos que acessam os espaços virtuais da Internet estejam informados sobre os riscos destes ambientes, além de informados quanto aos cuidados necessários para evitar exposições desnecessárias de suas vidas pessoais, em especial, entre os jovens, nativos digitais.

O ato da denúncia de um crime cibernético é igualmente importante porque, além de servir de registro estatístico para histórico, análises e tendências futuras, servirá

também para o devido enquadramento legal, a partir das informações registradas nos canais oficiais.

Totais Gerais dos Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos à Pornografia Infantil, Racismo e Homofobia.

Figura 21. Totais Gerais dos Indicadores Consolidados da Central Nacional de Denúncias de Crimes Cibernéticos relativos aos 3 crimes cibernéticos objetos da análise.



Fonte: Elaborado pela autora através de dados da SAFERNET, 2018.

Este gráfico fornece uma visualização ampliada sobre os dados relativos às denúncias dos crimes cibernéticos quanto aos números totais de denúncias feitas e registradas na Central Nacional de Crimes Cibernéticos, com a pornografia infantil liderando as denúncias feitas nos órgãos.

Por que denunciar?

Em 12 anos, a SaferNet recebeu e processou 3.925.405 denúncias anônimas, envolvendo 701.224 páginas (URLs) distintas escritas em 9 idiomas e hospedadas em 94.155 hosts diferentes, conectados à Internet através de 56.416 números IPs distintos, atribuídos para 101 países em 5 continentes.

Ajudou 15.983 pessoas em 27 unidades da federação e foram atendidos 2.269 crianças e adolescentes, 1.751 pais e educadores e 11.963 outros adultos em seu canal de ajuda e orientação.

Além disso, foram realizadas 570 atividades de sensibilização e formação de multiplicadores de 297 cidades diferentes, 27 estados, contemplando diretamente 22.325 crianças, adolescentes e jovens, 26.570 pais e educadores e 1.345 autoridades, com foco na conscientização para boas escolhas online e uso responsável da Internet.

Estas atividades beneficiaram mais de 1.2 milhões de pessoas indiretamente nas ações derivadas.

A denúncia dos crimes revela a importância desta ação, em função das providências judiciais que se seguem, podendo culminar nas penas e sanções cabíveis a cada caso, para criminosos e agressores.

A Organização das Nações Unidas (ONU) possui, igualmente, um canal de denúncia crimes e violações praticadas contra os Direitos Humanos. Por entender a importância e gravidade sobre o tema, o Conselho de Direitos Humanos e outros organismos da ONU que trabalham nesta área investigam violações de direitos humanos, quando são devidamente comprovadas e a investigação é realizada de forma confidencial.

> "O critério para aceitar uma denúncia está geralmente relacionado à credibilidade da fonte e da informação recebida, assim como aos detalhes proporcionados. Apesar disto, deve ser enfatizado que o critério em responder a uma denúncia individual varia, por isso é necessário que a

> comunicação seja submetida seguindo padrões estabelecidos.” (ONUBR, 2018b).

Uma denúncia pode evitar um crime, pode evitar uma morte ou suicídio, dependendo da tipificação do crime, do agressor, da vítima, e das consequências provenientes do crime.

3. EDUCAÇÃO E SEGURANÇA DIGITAL PARA UMA INTERNET MAIS SEGURA E DIREITOS HUMANOS NO MUNDO CIBERNÉTICO DOS JOVENS

Hoje presenciamos o despertar de uma verdadeira revolução tecnológica: inteligência artificial, blockchain, impressão 3D, robótica, Internet das Coisas, são alguns exemplos de tecnologias que já estão transformando a forma como vivemos, nos comunicamos, nos relacionamos e, em especial, a forma como aprendemos. O processo de aprendizagem é algo que precisa de constante aprimoramento, principalmente em se tratando dos dias atuais, no calor das grandes mudanças tecnológicas.

Neste contexto do processo de aprendizagem, vale a pena apresentar algo citado há quase duas décadas atrás, mas não menos importante. Trata-se de dizer que,

> Aprendizagens permanentes e personalizadas através de navegação, orientação dos estudantes em um espaço do saber flutuante e destotalizado, aprendizagens cooperativas, inteligência coletiva no centro de comunidades virtuais, desregulamentação parcial dos modos de reconhecimento dos saberes, gerenciamento dinâmico das competências em tempo real...esses processos sociais atualizam a nova relação com o saber. LÉVY (1999, p. 177)

Apesar do ano desta publicação – 1999 – ano que antecedeu ao surgimento e crescimento exponencial das redes sociais de hoje, o fenômeno das “árvores de conhecimento” foi algo idealizado por Pierre Lévy, como “crescendo a partir das autodescrições dos indivíduos, uma árvore de conhecimentos torna visível a multiplicidade organizada das competências disponíveis em uma comunidade”.

O fenômeno das “árvores de conhecimento” de Lévy teria sido um ensaio para a mudança de paradigma que a humanidade viveria nas décadas seguintes? Hoje, em pleno ano de 2018, século XXI, ainda estamos compreendendo as formas, velocidades e amplitudes da revolução tecnológica que já estamos passando. A 4ª Revolução Industrial.

Schwab (2016, p. 13) observa a respeito desta 4ª Revolução Industrial, caracterizada por três razões: velocidade – como resultado de um mundo profundamente interconectado, com novas tecnologias gerando outras tecnologias; amplitude e profundidade – que tem a revolução digital como base e combina várias tecnologias com mudanças consideráveis de paradigma; e impacto sistêmico – envolve a transformação de sistemas inteiros entre países e em toda a sociedade.

Basta um olhar mais cuidadoso para o mundo à nossa volta. Já percebemos consideráveis mudanças em nossas vidas que caracterizam a dita "4ª Revolução Tecnológica".

Silva (2015, p. 57) cita que

> antes de tudo, é fundamental compreendermos que toda ação educativa é sempre complexa e exige que atentemos para vários fatores. Sendo assim, ela não é influenciada somente pelos comportamentos individuais de quem a exerce – em especial, os pais e professores; os aspectos culturais e sociais também atuam profundamente no processo educativo e sobre a base biopsicológica de cada indivíduo.

No atual momento em que os indivíduos experimentam, a todo momento, novas formas de interação humana, através das diversas plataformas digitais, o processo de aprendizagem passa por mudanças significativas, onde é possível transmitir conteúdos, às novas gerações, de formas variadas. Sob este aspecto, Lilia Porto (2018, p. 5), num estudo chamado "Zeitgeist Aprendizagem 2018" citou que

> O futuro da aprendizagem será, ao mesmo tempo, tecnológico e afetivo, descentralizado e dialógico". Isto é incrivelmente encantador, do ponto de vista de colocar um olhar, tanto humano e tanto tecnológico, na educação e suas diversas possibilidades de aprendizagem, conjugando homem-máquina, numa forma tal que sejam explorados os benefícios proporcionados pelas máquinas, computadores, robôs, etc, para facilitar e melhorar aprendizados.

Porto (2018, p.5), ainda afirma que "De forma tímida, essas mudanças já estão sendo materializadas no Brasil, mas precisamos acelerar o passo para garantir que todas as crianças, os jovens e os profissionais brasileiros, sem exceção, tenham acesso a aprendizados alinhados aos desafios do futuro".

Ora, se considerarmos que já estamos vivendo um momento desafiador, cercados de uma gigantesca massa de dados desestruturados e distribuídos em diversas redes de computadores, fenômeno também conhecido como “Big Data”; se considerarmos também que estamos envoltos em tecnologias “vestíveis”, também conhecidos como “*wearables*” que promovem leituras e coletas de dados do corpo humano, através de sensores óticos que nos fornecem leituras gráficas sobre a saúde; se considerarmos, ainda, outras tantas tecnologias disruptivas já em uso, como a inteligência artificial, impressoras 3D, Internet das Coisas (IoT), Nanotecnologia, Blockchain e criptomoedas, podemos considerar que o mundo cibernético teve avanços profundos e consideráveis, com vistas a beneficiar a vida neste planeta.

Schwab (2016, p. 23), em seus ensaios para o “Fórum Econômico Mundial” de 2016, citou que “todas as inovações e tecnologias têm uma característica comum: elas aproveitam a capacidade de disseminação da digitalização e da tecnologia da informação”.

A revolução tecnológica vivida nos dias de hoje, inevitavelmente, faz uso de inovações tecnológicas nas mais variadas formas, nos mais variados conceitos, objetivos e benefícios a alcançar.

> Estamos no início de uma revolução que alterará profundamente a maneira como vivemos, trabalhamos e nos relacionamos. Em sua escala, escopo e complexidade, a quarta revolução industrial é algo que considero diferente de tudo aquilo que já foi experimentado pela humanidade. (Schwab, 2016, p. 11)

O “Fórum Econômico Mundial” que acontece todos os anos na cidade de Davos, na Suiça, promove um encontro de grandes líderes mundiais, chefes de Nações, acadêmicos, Presidentes de grandes organizações e especialistas de diversas áreas com objetivo de discutir questões importantes que afetam a humanidade no planeta Terra.

É uma organização internacional de cooperação público-privada que serve como plataforma global e visa identificar os grandes problemas que afetam a humanidade e buscar respostas aos grandes desafios. Sobre este aspecto, importante lembrar que

“A humanidade precisa de mentes mais abertas, escutas mais sensíveis, pessoas responsáveis e comprometidas com a transformação de si e do mundo”. (MORIN, 2011, p.13)

O compromisso de mudar e transformar, quando proveniente de uma ação conjunta de múltiplos atores, possibilita o alcance do sucesso. A educação do futuro deve nortear ações voltadas a saberes ligados ao preparo das mentes visando tempos incertos, inesperados, imprevistos. E isto é demasiado importante para o aprendizado de novos saberes do mundo digital.

> Independentemente de nossa consciência ou vontade, o futuro está sendo gestado e parido o tempo todo por todos nós, educadores profissionais ou não. Porém, se o quisermos de forma que seja um Futuro que proteja a Vida Coletiva e eleve e honre nossa dedicação profissional, precisamos repensar e refazer nossas práticas, isto é, nos novos tempos, novas atitudes! CORTELLA (2014, p. 11)

Conforme observado por CORTELLA, há pensamentos e discussões das mais variadas ordens a respeito da necessidade, emergente e constante, de renovação da educação...ter um olhar aprofundado sobre o futuro da educação, fazendo também um contraponto com as observações de MORIN (2011) em seu estudo “Sete Saberes Necessários para a Educação do Futuro”.

Após o surgimento das tecnologias de informação e comunicação, em dado momento, a educação, assim como em diversas outras áreas, passa a utilizá-las das mais variadas formas, como mencionam Conte & Fillippozzi Martini (2015, p. 1201)

> Daí a necessidade de buscar alternativas para utilizarmos as tecnologias como meio para fazer o sujeito pensar, educar-se e aprender com os outros nas múltiplas possibilidades de interação com o conhecimento. Interagindo com diferentes tempos de aprendizado, os sujeitos cada vez mais singulares, múltiplos e em meio à metamorfose (ou à aprendizagem) permanente, necessitam conviver com todos os espaços sociais e as mais recentes tecnologias.

Utilizar a tecnologia e suas diversas plataformas digitais como meio alternativo para ampliar o processo de aprendizagem é, sem dúvida, um meio de caminhar ao lado da modernidade que as tecnologias proporcionam. Porém, é importante considerar o uso seguro, ético e transparente dos meios digitais e, neste ponto, o papel da segurança

digital (também conhecido como cibersegurança) é fundamental, como citado por Shackelford (2017), onde ele diz que

> é hora de repensar o modo como entendemos a *cibersegurança* das comunicações digitais. Um dos principais defensores da liberdade de expressão nas Nações Unidas, o especialista em direito internacional David Kaye, pediu em 2015 que "a encriptação das comunicações privadas seja uma norma". Estes e outros incrementos nas comunidades internacionais e de negócios sinalizam o que poderiam ser as primeiras fases na declaração da *cibersegurança* como um direito humano que governos, empresas e indivíduos deveriam trabalhar para proteger.

A segurança digital (ou cibersegurança) é de fundamental importância para proporcionar ambientes tecnicamente mais seguros, com riscos e ameaças digitais minimizados, através da aplicação de ações aplicadas através de soluções tecnológicas de segurança.

Do mesmo modo, o uso de práticas seguras nos ambientes digitais pode minimizar vulnerabilidade digital de usuários da Internet. Estas práticas de segurança e ações educativas estão descritas e detalhadas em capítulo específico, através do conteúdo da cartilha "Orientações para uma Internet mais humana".

Educar em respeito aos Direitos Humanos Digitais, aqueles que devem ser preservados e respeitados no mundo digital da Internet, é de igual importância. Considerando a vida disseminada nas grandes redes, através da exposição, troca e compartilhamento de dados pessoais, é imperioso o respeito aos limites e vida pessoal de cada indivíduo, de qualquer ser humano.

Neste aspecto, e a respeito do uso de acesso dos jovens às plataformas digitais, Peck (2016, p. 525) cita que

> Com o atual cenário de uma sociedade cada vez mais digital, não há como se esquivar da necessidade de educar e orientar os jovens quanto às condutas também no ambiente virtual. Não basta apenas entregar, disponibilizar uma máquina para o aluno e ensiná-lo a utilizar suas diversas funções, se não aprenderem também que devemos zelar pela segurança digital, bem como agir de forma ética e legal, a fim de sermos bons cidadãos digitais.

Conforme esta abordagem, entende-se que educação digital e inclusão digital precisam caminhar lado a lado. A educação praticada hoje no mundo já conta com diversas e inúmeras tecnologias de informação e comunicação, através de plataformas digitais que proporcionam a inclusão de pessoas em zonas de habitação distantes das grandes cidades onde há dificuldade. Mas, não basta simplesmente "entregar" uma tecnologia a alguém, sem ao menos, instruí-la, incluí-la digitalmente. Neste sentido, Peck (2016, p. 526) segue afirmando que

> A educação digital deve ser promovida simultaneamente à inclusão digital dos usuários, seja dos indivíduos que estão tendo o primeiro contato com as máquinas somente no ambiente de trabalho, seja da nova geração que já nasceu dentro de uma sociedade totalmente informatizada. Este último grupo necessita de orientação especial, já que crianças e adolescentes estão passando pelo amadurecimento de seus conceitos éticos, morais e de cidadania.

A respeito da educação no mundo e das necessidades de sua expansão para que todo e qualquer ser humano tenha direito a ela, no ano de 2015, diversos Estados-membro das Organização das Nações Unidades, ao tratar do desenvolvimento de ações globais para o planeta, criaram 17 objetivos para transformar o mundo, acabar com a pobreza, promover prosperidade e bem-estar para todos, proteger o meio ambiente e enfrentar mudanças climáticas.

Também conhecidos como "Objetivos de Desenvolvimento Sustentável", representados na figura 19, Os 17 Objetivos de Desenvolvimento Sustentável e 169 metas anunciadas, demonstram a escala e a ambição desta nova agenda universal.

Eles se constroem sobre o legado dos Objetivos de Desenvolvimento do Milênio e concluirão o que estes não conseguiram alcançar. Eles buscam concretizar os direitos humanos de todos e alcançar a igualdade de gênero e o empoderamento das mulheres e meninas. Eles são integrados e indivisíveis, e equilibram as três dimensões do desenvolvimento sustentável: a econômica, a social e a ambiental.

A figura a seguir apresenta os "17 Objetivos de Desenvolvimento Sustentável" e seus respectivos temas, dando uma visão a cerca das propostas de ações que a Organização das Nações Unidas promovem e incentivam para o mundo até 2030.

Figura 22. Objetivos de Desenvolvimento Sustentável da ONU.

Fonte: ONUBR, 2015.

A respeito do tema da educação, o “Objetivo de Desenvolvimento Sustentável 4 (ODS 4) – Educação de Qualidade” visa “Assegurar a educação inclusiva e equitativa e de qualidade, e promover oportunidades de aprendizagem ao longo da vida para todos e todas”, considerando a vida vivida hoje num mundo digitalmente globalizado.

Sob a ótica da educação na atual sociedade digital, e considerando a importância do Objetivo de Desenvolvimento Sustentável 4, abordado acima, para educação e inclusão equitativa, Peck (2016, p. 527) afirma que

> Educar na sociedade digital não é apenas ensinar como usar os aparatos tecnológicos ou fazer efetivo uso da tecnologia no ambiente escolar. Educar é preparar indivíduos adaptáveis e criativos com habilidades que lhes permitam lidar facilmente com a rapidez na fluência de informações e transformações. É preparar cidadãos digitais éticos para um novo mercado de trabalho cujas exigências tendem a ser maiores que as atuais.

Sendo a meta da ONU, através do “Objetivo de Desenvolvimento Sustentável 4”, seja o de amparar todos os seres humanos em condições igualitárias de acesso à educação, ponto este já amparado pela “Declaração Universal de Direitos Humanos

(DUDH)" através de seu Artigo 26 que cita que "Todo ser humano tem direito à educação", entendo que trata-se de um esforço que a comunidade mundial deve exercer, nas metas da agenda até 2030, para que os objetivos sejam alcançados e os direitos humanos fundamentais sejam assegurados. Por vivermos, atualmente, numa sociedade digital, tema abordado em parágrafos anteriores, as mesmas garantias devem ser asseguradas no mundo digital, respeitando os direitos humanos digitais.

Às novas gerações que fazem uso intenso das tecnologias de informação e comunicação é importante considerar e incluir práticas e cuidados para sobrevivência no mundo digital. A educação pode combinar o uso correto e adequado das tecnologias e, igualmente, pode ser o veículo para disseminar conceitos de segurança digital. Os jovens, indivíduos em formação, são curiosos e ousados, carecem de acompanhamento e cuidado no acesso e uso das inúmeras plataformas existentes no mundo digital.

Neste contexto, vale lembrar uma passagem de um clássico da literatura infanto-juvenil que, de certa forma, apesar da ambientação acontecer no século XIX, metaforicamente é possível perceber as nuances do comportamento de um jovem em ambientes desconhecidos, motivados pelo ímpeto que a idade lhe oferece.

> Alice estava começando a ficar muito cansada de estar sentada ao lado de sua irmã e não ter nada para fazer: uma vez ou duas ela dava uma olhadinha no livro que a irmã lia, mas não via figuras ou diálogos nele e "para que serve um livro?", pensou Alice, "sem figuras nem diálogos?"
> [...] subitamente um coelho branco com olhos cor-de-rosa passou correndo perto dela.
> [...] Ardendo de curiosidade, ela correu pelo campo atrás dele, a tempo de vê-lo saltar para dentro de uma grande toca de coelho embaixo da cerca. No mesmo instante, Alice entrou atrás dele, sem pensar como faria para sair dali. A toca do coelho dava diretamente em um túnel, e então aprofundava-se repentinamente. Tão repentinamente que Alice não teve um momento sequer para pensar, antes de já se encontrar caindo, no que parecia ser bastante fundo". (CARROLL, 1865)

A ambientação do livro de CARROLL, "Alice no país das maravilhas" (1865), no século XIX, traz uma abordagem interessante a respeito do ímpeto de indivíduos em "lançar-

se” em ambientes desconhecidos, talvez movidos pela curiosidade, por impulso ou por querer descobrir algo desconhecido.

“[...] Alice não teve um momento sequer para pensar, antes de já se encontrar caindo, no que parecia ser bastante fundo”. O primeiro período da frase é o lançar-se para frente, para o desconhecido; o segundo período é a percepção do “onde estou”.

Trazendo esta metáfora para o mundo digital, indivíduos lançam-se rumo a ambientes digitais desconhecidos, conectam-se com pessoas desconhecidas, fornecem informações em demasia, acessam ambientes estranhos.

Similarmente a “Alice”, entedia-se com o igual, o imóvel, o livro “sem figuras e nem diálogos”, o mundo digital apresenta o novo, o dinâmico, a inovação, o movimento, a conexão.

Se neste ambiente digital e dinâmico que é a Internet, fruto de inúmeros espaços tecnológicos como redes sociais, jogos online, sites e blogs, entre outros, o uso for feito através dos chamados “nativos digitais”, indivíduos que nasceram num mundo tecnologicamente conectado, onde a Internet já caminhava a passos largos com seus diversos ambientes virtuais, certamente o números relativos a acesso e uso são grandes.

Investir na prevenção é importante para proteger quem sofre com o cyberbullying, alertando a sociedade sobre este fenômeno. Neste sentido, a Lei 12.965/2014, também conhecida como “Marco Civil da Internet” que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, destaca, em seu artigo 26, que é “dever constitucional do Estado na prestação da educação para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico” (Lei 12.965/2014, artigo 26).

> Assim, o universo tecnológico vem dando origem aos filhos da “cultura da simulação” que interagem com diferentes avatares para representá-los. Uma geração que vive imersa em diferentes comunidades de aprendizagem e que

> abre várias janelas ao mesmo tempo e resolve problemas fazendo "bricolagens", na medida em que organiza e reorganiza os objetos conhecidos sem um planejamento prévio. Nessa perspectiva, esses indivíduos – na maior parte das vezes, adolescentes e jovens – aprendem "futucando", uma característica que, cada vez mais, também vem sendo exercitada pelos adultos. ALVES (2007, p.147)

Nestas considerações feitas há 11 anos atrás, ALVES abordou algumas características dos jovens, "filhos da simulação", uma geração imersa em "diferentes comunidades de aprendizagem". São as perspectivas necessárias que a educação deve, a cada dia, reinventar-se num modo apropriado à ambientação da época em que se vive, proporcionando veículos de informação, para os nativos digitais, capazes de motivar, prender a atenção, instigar a curiosidade, enfim, mobilizando os sujeitos para o aprendizado de quaisquer conteúdos.

> Em geral, me consideram um otimista. Estão certos. Meu otimismo, contudo, não promete que a Internet resolverá, em um passe de mágica, todos os problemas culturais e sociais do planeta. Consiste apenas em reconhecer dois fatos. Em primeiro lugar, que o crescimento do ciberespaço resulta de um movimento internacional de jovens ávidos para experimentar, coletivamente, formas de comunicação diferentes daquelas que as mídias clássicas propõem. Em segundo lugar, que estamos vivendo a abertura de um novo espaço de comunicação, e cabe apenas a nós, explorar as potencialidades mais positivas deste espaço nos planos econômico, político, cultural e humano. LÉVY (1999, p.11)

Estas palavras, magistralmente colocadas por Lévy, no fim dos anos 90, já denotavam sua clareza de ideias e pensamentos, quanto ao futuro da cibercultura e seus efeitos benéficos à sociedade. Hoje, quase 20 anos depois, percebem-se os resultados de suas valiosas reflexões e o quanto ainda são atuais, considerando os grandes avanços alcançados pela sociedade digital e a cultura cibernética, promovidas, inclusive, pelo grande avanço e utilização das redes sociais entre os diferentes povos do mundo.

4. CARTILHA – “ORIENTAÇÕES PARA UMA INTERNET MAIS HUMANA”

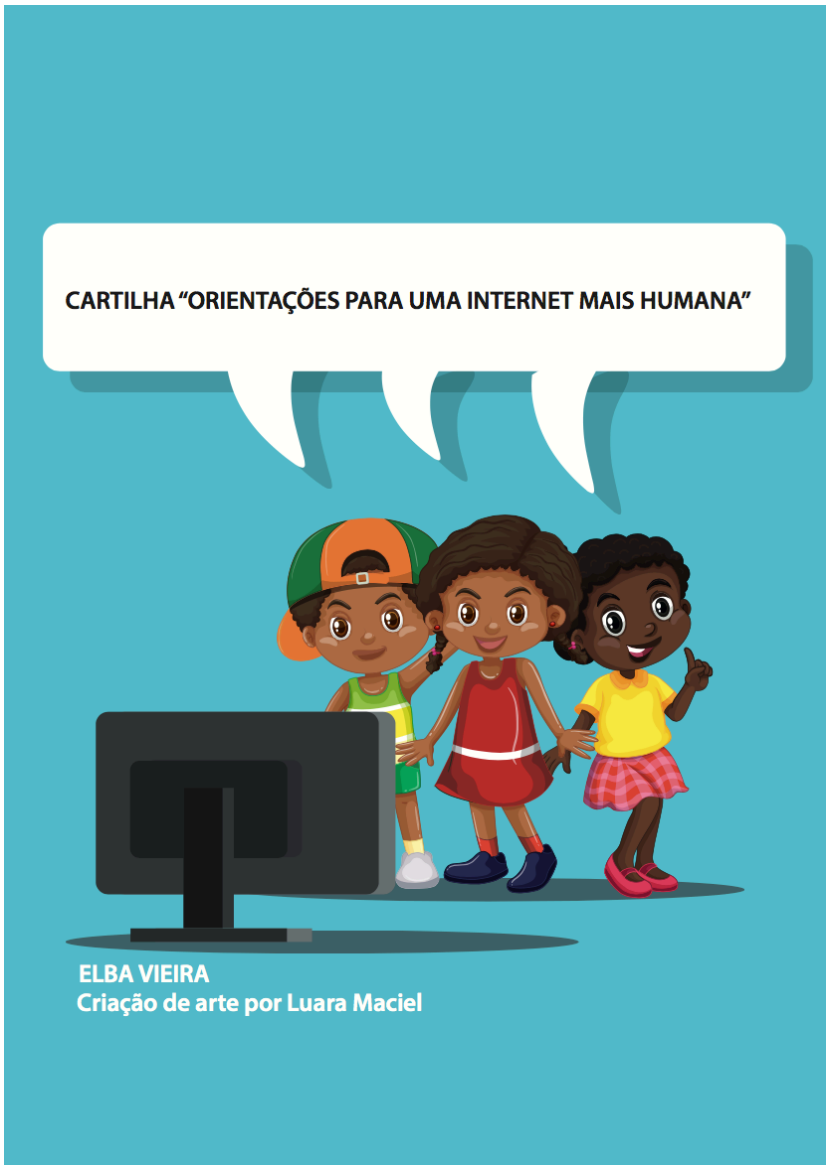
O Brasil, atualmente, passa por um momento de instabilidade política, em face do período de Eleições e da possibilidade de uma mudança substancial em quem irá ocupar o lugar da Presidência da República. Muitos movimentos sociais estão acontecendo nas ruas (físicas reais e digitais), demonstrando apreensão sobre o futuro próximo do país. O sentimento da pesquisadora é de que estamos passando por um grave momento, onde a ansiedade e o medo rondam os meios digitais e físicos, ante mudanças que podem afetar a vida das pessoas, a educação, saúde e outros aspectos e direitos já conquistados e alcançados.

“Esses momentos graves significam, como sempre na história humana, a possibilidade de momentos grávidos. Sim, momentos graves também são momentos grávidos! Afinal de contas, toda situação grave contém uma gravidez, ou seja, a possibilidade de dar à luz uma nova situação”. (CORTELLA, 2014, p. 10 e 11)

Como disse Cortella, “momentos grávidos” requerem a possibilidade de dar à luz uma nova situação. Seguindo este pensamento, uma das propostas desta pesquisa é apresentar uma cartilha com conteúdo educativo em segurança digital, referente ao Cyberbullying e dicas de segurança para serem utilizadas no meio digital.

Esta cartilha chama-se “Orientações para uma Internet mais humana”, conforme a capa apresentada na figura 20 e seu conteúdo está contido no “Apêndice A”.

Figura 23. Cartilha “Orientações para uma Internet mais humana”.



Fonte: elaborada pela autora.

5. CONSIDERAÇÕES FINAIS

A humanidade, após décadas de transformações no modo como se cria, manuseia e descarta informações, vive hoje numa sociedade digital. Indivíduos, nativos digitais ou não, já vivem num mundo conectado, 24 horas por dia, dependentes das tecnologias de informação e comunicação, materializadas por plataformas digitais utilizadas em diversos segmentos.

Neste mundo digital hiperconectado, assim como no mundo físico real, os direitos humanos precisam ser assegurados. Direitos Humanos Digitais devem ser respeitados nos diversos espaços digitais da Internet

Práticas como o Cyberbullying que precedem crimes nos espaços digitais, como foi abordado ao longo desta pesquisa, precisa ser entendido como uma prática criminosa. É preciso o envolvimento e participação ativa de vários atores no combate e enfrentamento desta prática. Acredito que esta luta é de todos e para todos.

Governos precisam ser mais enérgicos no combate à prática, com mais rigor, apoiando os órgãos policiais e de inteligência na busca e apreensão dos agressores que praticam crimes através da prática do Cyberbullying; na adoção de políticas públicas que incluam segurança digital como tema para ser conhecido, discutido e aplicado nas escolas, para que crianças e jovens possam crescer e desenvolver uma cultura digital incluída de práticas e cuidados seguros para sua sobrevivência nos espaços digitais, e também na capacitação de professores e gestores de escolas no aprofundamento do tema, para melhor preparar os jovens, através da educação.

Organizações (públicas e privadas) precisam ser mais enérgicas no apoio tecnológico, financeiro e de mão-de-obra especializada às Instituições (governamentais ou não governamentais) que lidam diariamente com vítimas ou testemunhas de agressões, denunciando práticas de Cyberbullying, acompanhadas de crimes digitais graves.

Instituições de ensino e escolas precisam ser mais enérgicas no fortalecimento de suas estruturas, cobrando Governos para o aprimoramento de ferramentas tecnológicas e na capacitação permanente de seu corpo de instrutores, gestores e professores no campo da segurança digital, para que tenham condições de transferir conhecimentos aos jovens, em especial. Além disso, ela mesma pode buscar apoio a outras Instituições na busca pelo conhecimento necessário às suas carências, relativas ao uso de tecnologias na educação, no conhecimento sobre segurança digital, e tantas outras.

A sociedade civil precisa ser mais enérgica no entendimento sobre o tema que rodeia o Cyberbullying e os crimes digitais praticados através dele, buscar e cobrar ações de Governos e acompanhar, atentamente, as atividades dos menos instruídos ou vulneráveis, a exemplo de crianças e jovens, nas plataformas digitais existentes na Internet. É preciso denunciar agressores, para que sejam tomadas as medidas jurídicas cabíveis aos responsáveis e criminosos.

Crimes (digitais ou não) não podem ficar impunes. É inaceitável o crescimento dos índices de casos de agressões digitais, com vítimas sofrendo sequelas nefastas, comprometendo a saúde mental que, muitas vezes, desencadeiam no suicídio.

Considero o Cyberbullying uma doença digital de âmbito social, em que afeta muitas pessoas e há responsabilidade de vários atores. Ações educativas em segurança digital podem servir de ferramentas de enfrentamento e combate ao cyberbullying. Por ser pesquisadora de um centro de pesquisa embasado em ações relacionadas à humanidades (CRDH – Centro de Referência e Desenvolvimento de humanidades), esta pesquisa e a cartilha elaborada “Orientações para uma Internet mais humana” é apenas uma contribuição desta especialista em segurança da informação, à comunidade, às escolas, à cidade e ao país, com o intuito de colaborar com a construção e manutenção de uma cultura digital segura para todos.

Torço, estudo, trabalho e incentivo ações por uma Internet mais ética, transparente e segura.

6. REFERÊNCIAS

AFFERO LAB, TORUS. **O futuro das coisas.** Zeitgeist Aprendizagem 2018. Disponível em: https://drive.google.com/file/d/1UZ8Fb7paABfQbNrg1e-1VU32FzlofjGw/view. Acesso em 19/10/2018.

ALVES, Lynn. **Geração digital native, cursos on-line e planejamento**. Um mosaico de ideias. Em Desenvolvimento sustentável e tecnologias da informação e comunicação. Antônio Dias Nascimento, Nadia Hage Failho, Tânia Maria Hetkowski, Organizadores. Salvador. EDUFBA, 2007.

BAMBRILLA, Ana. **Para entender a mídias sociais.** Licença Creative Commons. Disponível em: http://paraentenderasmidiassociais.blogspot.com.br/2011/04/download-do-ebook-para-entender-as.html. Acesso em 28/3/2017.

BARABÁSI, Albert-Lázló. **LINKED** - A nova ciência dos networks. São Paulo: Leopardo Editora, 2009, 256 p.

BAUMAN, Zygmunt. **Vigilância Líquida**. Rio de Janeiro: Zahar, 2013, 159 p.

BBC. **BBC News Brasil.** Disponível em: https://www.bbc.com/portuguese/noticias/2014/04/140403_bullying_suicidio_canada_fl . Acesso em 28/7/2018.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Subchefia para assuntos jurídicos, Casa Civil, Presidência da República, Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 9/4/2017.

BRASIL. **Lei n. 8.069,** de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Subchefia para Assuntos Jurídicos, Casa

Civil, Presidência da República, Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L8069.htm. Acesso em 9/4/2017.

BRASIL. **Lei n. 12.737,** de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Subchefia para assuntos jurídicos, Casa Civil, Presidência da República, Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 20/10/2016.

BRASIL. **Lei 12.965** de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet. Subchefia para Assuntos Jurídicos, Casa Civil, Presidência da República. Brasília, 5 de junho de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 9/4/2017.

BRASIL. **Lei n. 13.185** de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Subchefia para assuntos jurídicos, Casa Civil, Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13185.htm. Acesso em 2/4/2017017.

BRASIL. **Lei n. 13.709** de 14 de agosto de 2018. Dispõe sobre o tratamento de dados pessoais. Subchefia para assuntos jurídicos, Casa Civil, Presidência da República, Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 19/10/2018.

BRASIL. **O novo Banco de Desenvolvimento do BRICS.** Ministério das Relações Exteriores. Grupo dos G-20. Disponível em: http://www.itamaraty.gov.br/pt-BR/politica-externa/diplomacia-economica-comercial-e-financeira/118-g20. Acesso em 13/4/2017.

CÂMARA DOS DEPUTADOS. **Projetos de Lei e Outras Proposições**. Indicação ao Poder Executivo. INC 2231/2016. Sugere a promoção de ações voltadas para a incorporação transversal do tema Segurança Digital nos projetos pedagógicos das

escolas de ensino fundamental. Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2083386. Acesso em 20/1/2017.

CARROLL, Lewis. **Alice no País das Maravilhas**. 1865. Tradução: Clélia Regina Ramos. Petrópolis, RJ: Arara Azul, 2002. Disponível em: http://www.ebooksbrasil.org/adobeebook/alicep.pdf. Acesso em 29/4/2017.

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vítimas reais.** Rio de Janeiro: Brasport, 2014.

CASTELLS, Manuel. **A sociedade em rede.** Tradução: Roneide Venâncio Majer. 17ª ed. Revista e ampliada. São Paulo: Paz e Terra, 2016. 632 p.

CERF, Vinton. Internet access is not a human right. **New York Times,** 2012. Disponível em: http://www.nytimes.com/2012/01/05/opinion/internet-access-is-not-a-human-right.html. Acesso em 9/4/2017.

CGI.BR. **Princípios para a governança e uso da Internet**. São Paulo: Comitê Gestor da Internet no Brasil, 2009. Disponível em: https://cgi.br/media/docs/publicacoes/1/cgi-decalogo.pdf. Acesso em: 20/4/2016.

CHILDHOOD. Instituto WCF Brasil. **Navegar com Segurança.** Protegendo seus filhos da pedofilia e da pornografia infanto-juvenil na Internet. Disponível em: http://www.wcf.org.br/. Acesso em 20/10/2016.

COMSCORE. **Análises para um mundo digital.** Disponível em: http://www.comscore.com/por/. Acesso em 25/1/2017.

CONTE, Elaine; FILIPPOZZI MARTINI, Rosa Maria. As Tecnologias na Educação: uma questão somente técnica?. **Educação & Realidade,** v. 40, n. 4, Universidade Federal do Rio Grande do Sul. Porto Alegre, outubro-dezembro 2015. pp. 1191-1207. Disponível em: http://www.redalyc.org/articulo.oa?id=317241516013. Acesso em 17/4/2017.

CORTELLA, Mario Sérgio. **Educação, escola e docência.** São Paulo: Cortez. 2014. 126 p.

CORTELLA, Mario Sérgio. **Qual é a tua obra?** Inquietações propositivas sobre gestão, liderança e ética. São Paulo: Vozes. 2013. 141 p.

CRDH. Centro de Referência em Desenvolvimento e Humanidades. Disponível em: http://crdhbr.blogspot.com.br/p/inicio.html. Acesso em 21/4/2017.

Decision Report. Disponível em: http://www.decisionreport.com.br. Acesso em 30/7/2016

ISTART. **Família mais segura na Internet.** Disponível em: http://www.familiamaissegura.com.br/. Acesso em 2/11/2016.

FAMILIAMAISSEGURA. Família mais segura. Ética e segurança digital. Cartilha orientativa. Recomendações e dicas para a família sobre o uso correto das novas tecnologias. Disponível em http://www.familiamaissegura.com.br/wp-content/uploads/2014/01/Cartilha-Orientativa.pdf . Acesso em 28/7/2018.

FIORILLO, Celso Antonio Pacheco. **O Marco Civil da Internet e o meio ambiente digital na sociedade da informação:** Comentários à Lei n. 12.965/2014. São Paulo. Saraiva, 2015. 120 p.

G1. **Portal de notícias da Globo.** Disponível em: http://g1.globo.com/sp/sao-carlos-regiao/noticia/2016/05/jovem-emagrece-e-sofre-cyberbullying-ao-postar-foto-antiga-com-180-kg.html . Acesso em 28/7/2018.

GABRIEL, Martha. **Educ@r.** A (r)evolução digital na educação. São Paulo: Saraiva, 2013. 241 p.

GABRIEL, Martha. **Você, eu e os robôs.** Pequeno manual do mundo digital. São Paulo: Atlas, 2018.

GREENWALD, Glenn. **Sem lugar para se esconder.** Edward Snowden, a NSA e a espionagem do governo americado. “No place to ride”. Tradução de Fernanda Abreu. Rio de Janeiro: Sextante, 2014. 288 p.

HETKOWSKI, Tânia Maria; FIALHO, Nadia Hage; NASCIMENTO, Antonio Dias. Org. **Desenvolvimento sustentável e tecnologias de informação e comunicação.** Salvador: EDUFBA, 2007.

IEAFP. **Portal de Notícias.** Disponível em: http://www.iefap.com.br/noticia/10-casos-de-bullying-que-tiveram-consequencias-graves . Acesso em 28/7/2018.

LÉVY, Pierre. **Cibercultura.** São Paulo: Editora 34, 1999. 250 p.

LÉVY, Pierre. **A ideografia dinâmica.** São Paulo: Loyola, 2004. 231 p.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas, 2003.

MELLO, Mario. **Os smartphones estão se tornando o controle remoto do mundo**. ProXXima, 26 de janeiro de 2017. Disponível em: http://www.proxxima.com.br/home/proxxima/noticias/2017/01/26/os-smartphones-estao-se-tornando-o-controle-remoto-do-mundo.html. Acesso em 13/4/2017.

NUCCIBER. **Cuidado! Você pode estar agindo assim na internet.** Núcleo de Combate aos Crimes Cibernéticos, Ministério Público do Estado da Bahia. Disponível na Internet em: http://www.nucciber.mpba.mp.br/. Acesso em 25/10/2016.

MITNICK, Kevin; SIMON, William L. **A arte de enganar.** Ataques de hackers: controlando o fator humano na segurança da informação. Tradução: Kátia Aparecida Roque. São Paulo: Pearson Education do Brasil, 2003. 284 p.

MORIN, Edgar. **Os sete saberes necessários à educação do futuro.** Tradução de Catarina Eleonora F. da Silva e Jeanne Sawaya. 2. ed. São Paulo: Cortez; Brasília, DF; UNESCO, 2011. 102 p.

NAÇÕES UNIDAS NO BRASIL. **UIT** – União Internacional de Telecomunicações. Disponível em: https://nacoesunidas.org/agencia/uit/. Acesso em 21/4/2017.

NETHICS. Conhecendo Bullying e Cyberbullying. Disponível em https://nethicsedu.com.br/wp-content/uploads/2016/02/Cartilha-de-Bullying-e-Cyberbullying.pdf . Acesso em 28/7/2018.

NIC.BR. **Internet segura.** Disponível em: http://internetsegura.br/iniciativas-e-campanhas/. Acesso em 2/11/2016.

NOVAES, Ivan Luiz. **Construção do projeto de pesquisa sobre políticas e gestão educacionais.** Salvador: Eduneb, 2014. 122 p.

Observatório da Internet no Brasil. Disponível em: http://observatoriodainternet.br/. Acesso em 21/4/2017.

ONU. **Declaração Universal dos Direitos do Homem.** Organização das Nações Unidas, 10 de dezembro de 1948. Disponível em: https://www.pcp.pt/actpol/temas/dhumanos/declaracao.html. Acesso em 21/4/2017.

ONUBR. **17 objetivos para transformar nosso mundo.** Nações Unidas no Brasil, 2015. Disponível em: https://nacoesunidas.org/pos2015/. Acesso em 9/4/2018.

ONUBR. **O que são os direitos humanos?** Nações Unidas no Brasil, 2018a. Disponível em: https://nacoesunidas.org/direitoshumanos/. Acesso em 9/4/2018.

ONUBR. **Como denunciar violações de direitos humanos à ONU.** Nações Unidas no Brasil, 2018b. Disponível em: https://nacoesunidas.org/direitoshumanos/denuncias/. Acesso em 9/4/2018.

PARAÍBA. **Bullying não é brincadeira.** Promotoria da Infância e Juventude, Ministério Público do Estado da Paraíba, João Pessoa, 2009. Disponível em: https://new.safernet.org.br/sites/default/files/content_files/cartilha_bullying.pdf.
Acesso em 13/10/2018.

PECK, Patrícia Pinheiro. **Direito digital.** 6. ed. Rev., atual. e ampl. - São Paulo: Saraiva, 2016. 781 p.

PESSOA, Marcos Paulo et al. **A juventude conectada** – um estado da arte. em jogos eletrônicos, mobilidades e educações. Lynn Alves e Jesse Nery, Organizadores. Salvador. EDUFBA, 2015.

PORVIR. **Iniciativa de comunicação e mobilização social.** Disponível em: http://porvir.org/. Acesso em 4/8/2016.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico** [recurso eletrônico]: métodos e técnicas da pesquisa e do trabalho acadêmico. 2. ed. Novo Hamburgo: Feevale, 2013.

PRETTO, Nelson De Luca. **Reflexões: ativismo, redes sociais e educação**. Salvador. EDUFBA. 2013. 252 páginas.

RECUERO, Raquel & BASTOS, Marcos & ZAGO, Gabriela. **Análise de Redes para Mídia Social.** Ed.1, 2015, 182p.

RIOS, Terezinha Azerêdo. **Ética e competência**. Ed. Cortez. 2011. 20ª. Edição. São Paulo. 128 páginas.

ROCHA, José Cláudio. **Direitos humanos e a diversidade do mundo contemporâneo.** Revista Jus Navigandi, Teresina, ano 19, n. 3860, 25 jan. 2014. Disponível em: <https://jus.com.br/artigos/26503>.
Acesso em 5/1/2017.

ROCHA, José Cláudio. **Indústrias criativas e desenvolvimento humano, econômico, social e sustentável**. Revista Jus Navigandi, Teresina, ano 19, n. 3896, 2 mar. 2014. Disponível em: <https://jus.com.br/artigos/26514>.
Acesso em 5/1/2017

SAFE AND SECURE ONLINE. Cyber education & digital citizenship. 2016. Disponível em: https://safeandsecureonline.org/. Acesso em 30/7/2016

SAFERNET. **Cyberbullying.** S/D. Disponível em: https://new.safernet.org.br/node/163. Acesso em 1/11/2016.

SAFERNET. Safer Dicas. Brincar, estudar e...Navegar com segurança na Internet. Disponível em: https://new.safernet.org.br/sites/default/files/content_files/cartilha-saferdicas.pdf . Acesso em 28/7/2017.

SAFERNET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernéticos.** 2015. Disponível em http://indicadores.safernet.org.br/. Acesso em 1/11/2016.

SANTANA, Edésio T. **Bullying e cyberbullying:** agressões dentro e fora das escolas: teoria e prática que educadores e pais devem conhecer. São Paulo: Paulus, 2013.

SANTOS, Boaventura de Sousa; CHAUÍ, Marilena. **Direitos humanos, democracia e desenvolvimento.** São Paulo: Cortez, 2013. 133 p.

SCHACKELFORD, Scott. **A cibersegurança deveria ser um direito humano?** Tradução de Camilo Rocha. NEXO, 21 mar. 2017. Disponível em: https://www.nexojornal.com.br/externo/2017/03/21/A-ciberseguran%C3%A7a-deveria-ser-um-direito-humano. Acesso em 21/3/2017.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução: Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003. 156 p.

SILVA, Ana Beatriz Barbosa. **Bullying: mentes perigosas nas escolas**. [2. Ed.] - São Paulo: Globo, 2015. 206 p.

TAKAHASHI, Tadao. Org. **Sociedade da informação no Brasil.** Livro Verde. Brasília. Ministério da Ciência e Tecnologia. 2000. Disponível em: www.governoeletronico.gov.br/documentos-e-arquivos/livroverde.pdf. Acesso em 21/1/2017.

TECHNOBLOG. **Portal de Notícias.** Disponível em: https://tecnoblog.net/116422/cyberbullying-amanda-todd/ . Acesso em 28/7/2018.

TED. **Ideas worth spreading.** Disponível em: https://www.ted.com/talks/monica_lewinsky_the_price_of_shame?language=pt-br#t-10430 . Acesso em 28/7/2018.

THIOLLENT, Michel. **Metodologia da pesquisa-ação.** São Paulo: CORTEZ. 1986. 252 p.

Universidade do Estado da Bahia. Mestrado profissional "Gestão e Tecnologias Aplicadas à Educação (GESTEC). Apresentação e Regimento. Disponível em: http://www.uneb.br/gestec/sobre/. Acesso em 21/4/2017.

United Nations Human Rights. Office of the high commissioner. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em 13/10/2018.

VALENTE, Mariana Giorgetti et al. **O corpo é o código:** estratégias jurídicas de enfrentamento ao revenge porn no Brasil. São Paulo: InternetLab, 2016.

VIEIRA, Elba. **A gaveta do meio.** São Paulo: Scortecci, 2009. 84 p.

GLOSSÁRIO

AVATAR – figuras criadas à imagem e semelhança do usuário, utilizado em jogos de computador e ambientes virtuais.

BLOCKCHAIN – tradução para “cadeia de blocos”. É também conhecido como um protocolo de confiança e tem a função de criar um índice global de transações em determinados mercados. É considerada uma tecnologia disruptiva que cria consenso e confiança na comunicação direta entre duas partes, sem o intermédio de terceiros.

BIG DATA – refere-se a um volume muito grande de dados armazenados, geralmente de forma não estruturada.

BULLYING - intimidação sistemática; 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 (LEI 13185, 2015).

CRIPTOMOEDAS – é uma “moeda digital” que faz uso da tecnologia do Blockchain e da criptografia para assegurar validade de transações.

CYBERBULLYING – “bullying cybernético”. Intimidação sistemática na rede mundial de computadores, quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial (LEI 13185, 2015).

CYBERSEGURANÇA – “segurança cibernética”. Ver “Segurança Digital”.

DATA CENTER – centro de dados. Ambiente físico para guarda e armazenamento de equipamentos de tecnologia para realizar processamento, armazenamento e conectividade de dados e informações de empresas (públicas ou privadas).

GAMERS – jogadores de jogos eletrônicos.

HACKER – indivíduo fanático por computação, especializado em desvendar enigmas e códigos de acesso a computadores. Pode ser caracterizado como um “pirata” de computador que invade redes e sistemas para obter alguma vantagem.

IoT – “Internet of Things” que é a tradução para “Internet das Coisas”. Refere-se a rede de objetos físicos, a exemplo de veículos, equipamentos eletrônicos domésticos, dispositivos médicos, entre outros que possuem tecnologia embarcada, sensores e conexão com a rede, capazes de coletar e transmitir dados.

NANOTECNOLOGIA – manipulação da matéria numa escala mínima, atômica e molecular. Pode ser utilizada para criação de componentes a serem utilizados em diversas áreas, como na saúde, educação, física, química, entre outras.

NATIVO DIGITAL – indivíduo que nasceu e cresceu com as tecnologias digitais presentes em sua vida.

NOTEBOOK – computador portátil móvel.

REVENGE PORN – pornografia da vingança.

SEGURANÇA DIGITAL – conjunto de tecnologias, métodos e práticas, visando a proteção de um indivíduo, empresa, comunidade, organização ou país, no mundo digital da Internet e redes tecnológicas.

SEXTING – contração de “sex” e “texting”. É um anglicismo, referindo-se a divulgação de conteúdos eróticos e sensuais através do uso de celulares.

SMARTPHONE – telefone celular inteligente.

TABLET – computador móvel.

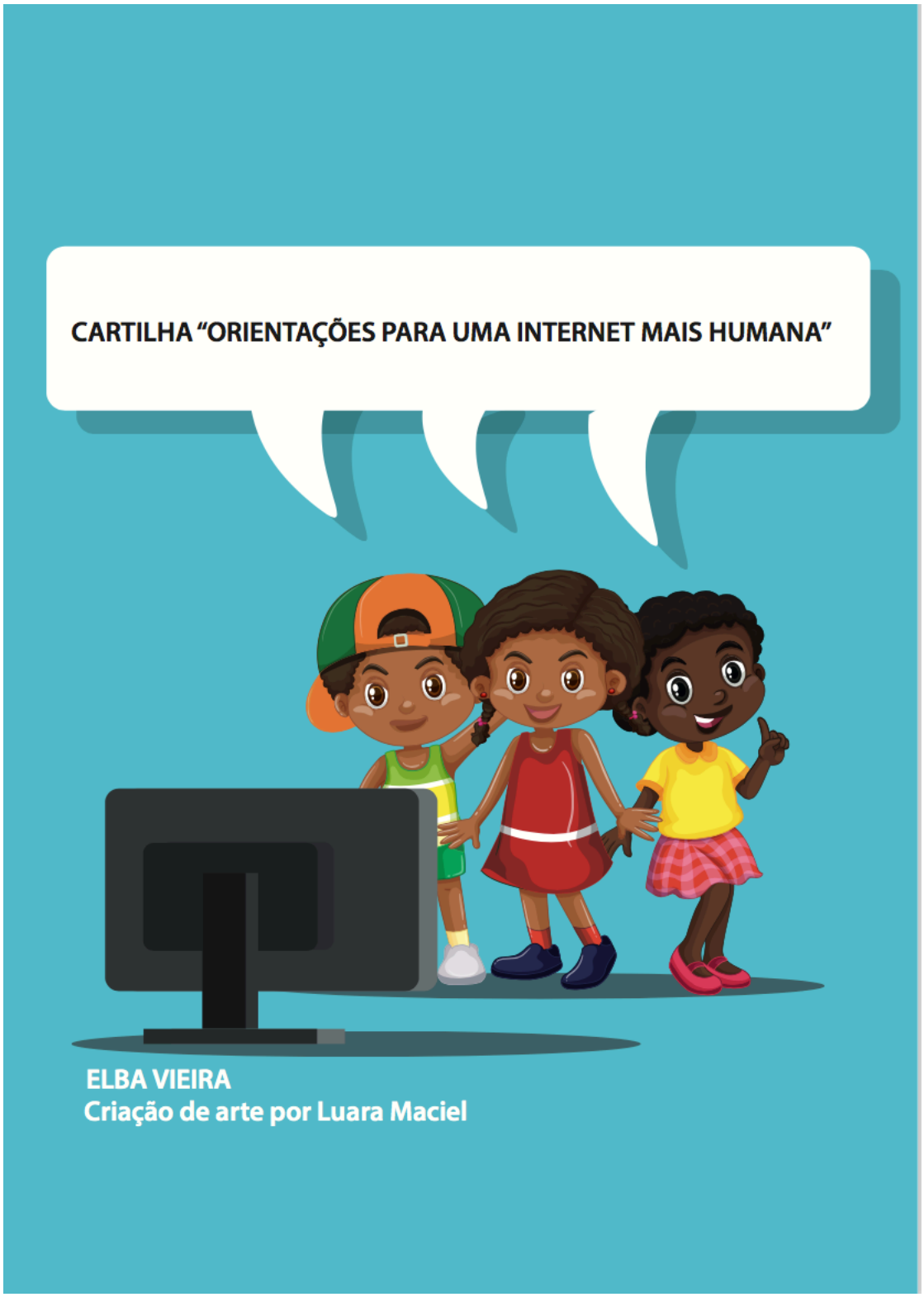
URL – “Uniform Resource Locator” traduzindo para Localizador Uniforme de Recursos. É um endereço de rede no qual se encontra algum recurso informático.

WEB – palavra inglesa que se refere à teia ou rede. Popularmente é utilizada para referir-se à Internet.

WEARABLE – tradução de “vestível”. Refere-se a tecnologias embarcadas em dispositivos “vestíveis”, a exemplo de relógios, pulseira inteligentes, óculos, roupas, etc.

APÊNDICE A

CARTILHA "ORIENTAÇÕES PARA UMA INTERNET MAIS HUMANA"



UNEB
Reitor: José Bites de Carvalho
Pró-Reitor: Marcelo Duarte Dantas de Avila
Coordenador do CRDH (Centro de Referência e Desenvolvimento em Humanidades): Prof. Dr. José Cláudio Rocha

SUMÁRIO

NOSSOS OBJETIVOS

Promover um olhar sobre o Bullying cibernético, também conhecido como Cyberbullying e sensibilizar famílias, educadores, governos, profissionais de diversas áreas e a sociedade civil, a respeito desta prática, abordando informações que podem ser úteis na identificação de casos de Cyberbullying.
A cartilha fornece dicas de segurança digital para despertar nas pessoas os cuidados necessários no uso dos ambientes digitais e ajudando na construção de uma Internet mais ética, segura e humana.

VOCÊ SABE O QUE É CYBERBULLYING?

O Cyberbullying é a versão virtual do Bullying, considerando que a prática ocorre no espaço da rede mundial de computadores (Internet). Esse fenômeno preocupa especialistas e educadores, por seu efeito multiplicador do sofrimento das vítimas e pela velocidade com que estas informações são veiculadas.
As modernas plataformas tecnológicas são os instrumentos utilizados para disseminar o Cyberbullying, prática com intuito de maltratar, humilhar ou constranger, sendo uma forma de ataque perverso, ganhando dimensões incalculáveis nas redes sociais, comunicadores instantâneos, chats, games, entre outras formas de comunicação digital.
Cyberbullying é um conjunto de comportamentos agressivos, intencionais e repetitivos que são adotados por um ou mais indivíduos contra outro indivíduo (ou grupo) e, na maioria dos casos, as práticas acontecem entre os jovens. O agressor insulta, espalha rumores e boatos sobre seus colegas, amigos ou familiares, até mesmo sobre os profissionais nas escolas.
O Decreto Federal 13.185 (6/11/2015) diz que Cyberbullying é "uma intimidação sistemática na rede mundial de computadores, quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial."

Este decreto foi criado para prevenir e combater a prática da intimidação sistemática em toda a sociedade. Isto vale para o Bullying e o Cyberbullying.
"A construção de uma sociedade justa e menos desigual só será possível se cada indivíduo possuir dentro de si, como valor maior, a busca incessante pela justiça e pelo respeito à dignidade humana. O enfrentamento à prática do bullying é uma importante colaboração na construção de uma sociedade diferente!"
(Alley Borges Escorel / Promotor de Justiça - MP/PB)

QUAIS OS TIPOS MAIS COMUNS DE CYBERBULLYING?

a) Flaming – Envio de mensagens vulgares ou que mostram hostilidade em relação a uma pessoa.

b) Agressão On-line – envio repetido de mensagens ofensivas.

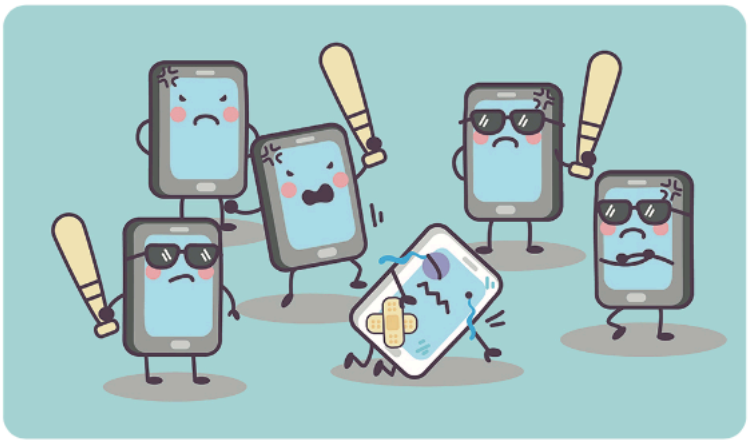
c) Cyberstalking – agressão on-line que inclui ameaças de dano ou intimidação excessiva.

d) Difamação – Envio de mensagens para terceiros ou postagem de comentários em ambiente digital, de caráter prejudicial, com informações falsas e afirmações cruéis sobre uma pessoa.

e) Substituição ilegal de uma pessoa – fazer-se passar pela vítima e enviar ou postar arquivos de texto, vídeo ou imagem que difamem o agredido.

f) Outing – enviar ou postar material sobre uma pessoa contendo informação sensível, privada ou constrangedora, incluídas respostas de mensagens privadas ou imagens.

g) Exclusão – cruel expulsão de alguém de um grupo on-line.



QUAIS SÃO OS AGENTES ENVOLVIOS NA PRÁTICA DO CYBERBULLYING?

a) Vítimas – São as pessoas que sofrem com o Cyberbullying.

b) Agressores - São pessoas que não respeitam as diferenças alheias e se aproveitam de suas fragilidades para fazer gozações e humilhações.

c) Testemunhas – São pessoas que não sofrem nem praticam o cyberbullying, mas convivem ou presenciam o problema e se omitem por medo e/ou insegurança. Acabam sendo cúmplices da situação.

ALGUMAS DICAS DE SEGURANÇA RELATIVAS AO CYBERBULLYING

a) Caso você tenha sido vítima de cyberbullying, guarde todas as evidências do agressor, podendo ser email, mensagens, áudios ou vídeos em alguma rede social, chats, games ou qualquer coisa que evidencie a agressão online deve ser preservada para facilitar a identidade do agressor.

b) Quebre o silêncio, denuncie a agressão que você sofreu para seus pais, responsáveis, professores na escola ou alguém que você confie. É importante que o agressor não cometa mais este tipo de prática.

c) Se algum amigo (a), familiar ou colega na sua escola sofreu agressão digital, converse com ele(a) para quebrar o silêncio e conversar com algum adulto, pais, responsáveis ou professores. Ofereça apoio e mostre que ele não está sozinho, nem é culpado pelas ofensas que está sofrendo.

d) Não seja um agressor virtual. Não pratique nenhum tipo de violência a amigo, colega, familiar, professor ou qualquer outra pessoa. Procure divulgar práticas positivas na Internet.

e) Não responda às provocações, se necessário, bloqueie quem estiver incomodando você. Converse com seus pais, responsáveis, professores ou alguém que você confie.

f) Os pais podem ser responsabilizados judicialmente pelas agressões que os filhos cometem. O mais adequado é tentar resolver essa situação com diálogo e orientação, já que crianças e adolescentes precisam do cuidado dos adultos, de ambos os lados da questão (vítimas e agressores).

ATENÇÃO!

O QUE FAZER E ONDE BUSCAR AJUDA PARA VÍTIMAS E TESTEMUNHAS DE CYBERBULLYING

a) Se você é vítima, peça ajuda. Mesmo sendo apenas pela Internet, é possível encontrar o responsável pela violência.

b) Guarde todas as provas que puder: fotos, e-mails, mensagens, áudios, vídeos, número de celular, informações do grupo de comunicadores instantâneos ou qualquer outro aplicativo, imagem de telas, etc

c) Nos casos de infrações contra a honra – calúnia, difamação e injúria – a vítima deve imprimir as páginas, e-mails, mensagens onde foram publicadas as ofensas para servirem de prova na abertura de procedimento na Justiça.

d) Alguns sites que podem oferecer apoio:

I. Família mais segura – www.familiamaissegura.com.br
II. Ministério Público da Bahia – Núcleo de Combate aos Crimes Cibernéticos (NUCCIBER)
III. Nethics – www.nethicsedu.com.br
IV. SAFERNET - https://new.safernet.org.br/helpline

DICAS GERAIS DE SEGURANÇA PARA USO DA INTERNET

a) Tenha bons hábitos online e não responda links anexados a e-mails não solicitados ou nas redes sociais.

b) Não forneça seus dados pessoais a quem você não conhece, seja por telefone, pessoalmente ou através de alguma plataforma digital.

c) Proteja suas senhas dos ambientes digitais que você acessa e utiliza.

d) Use senhas fortes, com mínimo de 8 caracteres, misturando letras, números e caracteres especiais.

e) Evite usar a mesma senha para várias contas.

f) Nunca passe senhas para outras pessoas, nem como prova de amor ou amizade.

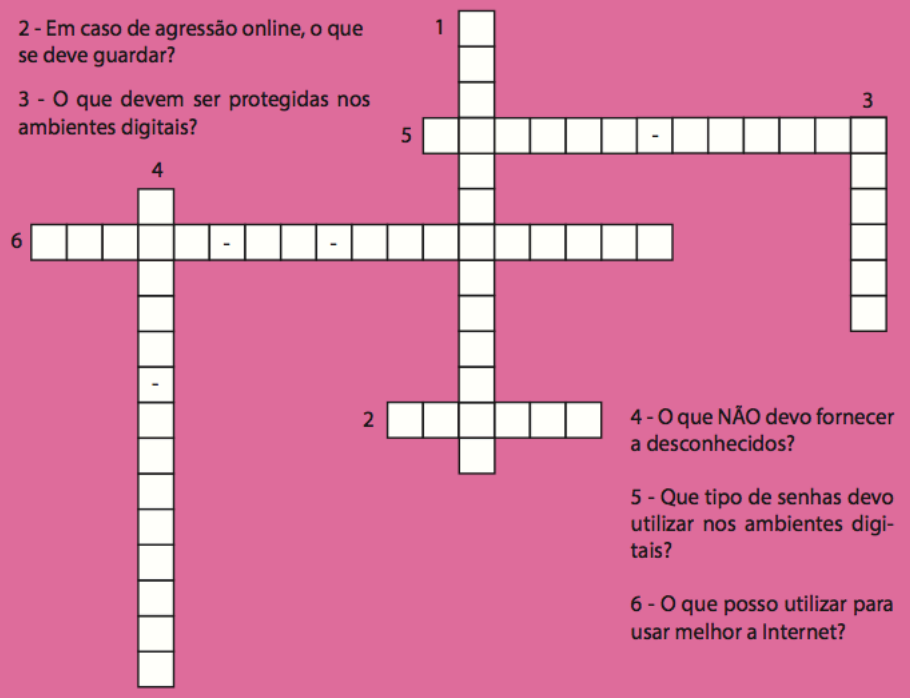
g) Cuidado com o que escreve e com as imagens que divulga na rede. Conecte-se com respeito.

PALAVRA CRUZADA

1 - Versão virtual do bullying

2 - Em caso de agressão online, o que se deve guardar?

3 - O que devem ser protegidas nos ambientes digitais?



4 - O que NÃO devo fornecer a desconhecidos?

5 - Que tipo de senhas devo utilizar nos ambientes digitais?

6 - O que posso utilizar para usar melhor a Internet?

Respostas:
1 - Cyberbullying
2 - Provas
3 - Senhas
4 - Dados Pessoais
5 - Senhas Fortes
6 - Dicas de segurança

Cyberbullying não é brincadeira! Só é brincadeira quando todos os envolvidos se divertem.

Acreditamos em ações para uma Internet mais segura, ética e humana!

REFERÊNCIAS

a) Família mais segura – www.familiamaissegura.com.br

b) Ministério Público da Bahia – Núcleo de Combate aos Crimes Cibernéticos (NUCCIBER)

c) Nethics – www.nethicsedu.com.br

d) SaferNet. www.safernet.org.br

e) Ministério Público da Paraíba.

f) ROCHA, Telma Brito. Cyberbullying: ódio, violência virtual e profissão docente. Brasília: Liber Livro, 2012. 192p.

g) SANTANA, Edésio T. Bullying e Cyberbullying: agressões dentro e fora das escolas: teoria e prática que educadores e pais devem conhecer. São Paulo: Paulus, 2013.

IMAGENS

Vetores retirados do FREEPIK e modificados

https://now.symassets.com/content/dam/norton/global/images/non-product/blog/types-of-cyberbullying.jpg