UNIVERSIDADE MUNICIPAL DE SÃO CAETANO DO SUL

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA

PROGRAMA DE PÓS-GRADUAÇÃO EM COMUNICAÇÃO

MESTRADO PROFISSIONAL EM INOVAÇÃO NA COMUNICAÇÃO DE INTERESSE PÚBLICO

CIRO FERREIRA DA SILVA JUNIOR

CIDADANIA DIGITAL NA PREVENÇÃO DE *CIBERBULLYING*

São Caetano do Sul

2020

CIRO FERREIRA DA SILVA JUNIOR

CIDADANIA DIGITAL NA PREVENÇÃO DE *CIBERBULLYING*

Dissertação apresentada ao Programa de Pós-Graduação em Comunicação da Universidade Municipal de São Caetano do Sul, como requisito parcial para obtenção do título de Mestre em Comunicação.

Área de concentração: Inovação na Gestão e Produção da Comunicação de Interesse Público

Linha de Pesquisa: Gestão da Comunicação de Interesse Público

Orientadora: Profa. Dra. Regina Rossetti

São Caetano do Sul

2020

FICHA CATALOGRÁFICA

JUNIOR, Ciro Ferreira da Silva.

Cidadania Digital na Prevenção de *Ciberbullying* / Ciro Ferreira da Silva Junior – São Caetano do Sul - USCS, 2020. 105f.
Orientadora: Regina Rossetti.
Dissertação (Mestrado) – USCS, Universidade Municipal de São Caetano do Sul, Programa de Mestrado Profissional em Comunicação, 2020.
1. Cidadania Digital 2. Proteção de Dados e Privacidade 3. *Ciberbullying* 4. Educação Digital 5. *Cibercrimes* 6. Comunicação de Interesse Público

I Cidadania Digital na Prevenção de *Ciberbullying* II Universidade Municipal de São Caetano do Sul

Reitor da Universidade Municipal de São Caetano do Sul
Prof. Dr. Leandro Campi Prearo

Pró-reitora de Pós-graduação e Pesquisa
Profa. Dra. Maria do Carmo Romeiro

Gestão do Programa de Pós-graduação em Comunicação
Prof. Dr. João Batista Cardoso

Trabalho Final de Curso defendido e aprovado em 26/11/2020 pela Banca Examinadora constituída pelos professores:

Profa. Dra. Regina Rossetti (USCS)

Prof. Dr. Alan César Belo Angeluci (USCS)

Prof. Dr. Vitor Souza Lima Blotta (USP)

Em primeiro dedico este trabalho acadêmico a Deus, posteriormente a minha querida esposa Glaucia Bambirra, as minhas duas filhas maravilhosas Mariana e Beatriz, como também as duas enteadas Letícia e Laura, incluindo as demais pessoas que fazem parte do meu convívio no dia a dia.

Combati o bom combate, acabei a carreira, guardei a fé – (II Timóteo, Capítulo 4, verso nº 7).

AGRADECIMENTOS

Primeiramente agradeço a Deus pela saúde em época de pandemia da Covid-19, incluindo também minha família, meu trabalho, pelo lar de paz, bem como pela enorme disposição pessoal, a fim de poder concluir este árduo trabalho acadêmico, no qual coloquei tamanho empenho, esforço, dedicação e disciplina, tudo para que fosse concretizada mais essa missão escolar com êxito e louvor.

É claro que não posso deixar de comentar a louvável e sincera contribuição da minha esposa Glaucia Bambirra Silveira, que inclusive é Doutoranda em Administração na USCS, nesse longo e rigoroso processo universitário que envolveu o Mestrado Profissional em Inovação na Gestão e Produção da Comunicação de Interesse Público da Universidade Municipal de São Caetano do Sul.

Lembro oportuno e conveniente a gratidão sempre relevante pelas minhas duas filhas, Mariana Primitz Silva, de 20 anos de idade e Beatriz Bambirra Silveira Silva, de 9 anos, pessoas realmente importantes no cenário de um pai preocupado e presente que proponho ser diariamente na vida de ambas, pois as duas trazem verdadeiramente para o meu ser, um prazer todo especial de viver e principalmente ao acordar todos dias de manhã.

Convém lembrar da minha mãe Mariana Regina da Silva, *in memoriam*, mas que na verdade sempre atuou de maneira ímpar na minha vida e formação acadêmica, bem como de meus irmãos, pois segundo seus dizeres o conhecimento enaltece, engrandece o ser humano e o difere de um simples homem médio.

A Senhora Regina como era conhecida no meio social, foi uma mulher muito forte, honesta, bastante religiosa, com valores éticos e morais exaltados e reconhecidos por terceiros, pois sempre respeitou a dignidade da pessoa humana de outros indivíduos, além de ser uma docente fervorosa por profissão. Tudo aquilo que se propôs a desenvolver durante a sua vida o fez com disciplina, amor e respeito ao próximo, porque sempre acreditou na carreira de professora, mesmo em tempos de dificuldade, porque ensinou e transmitiu a arte do conhecimento sempre com maestria.

Outro genuíno agradecimento se refere a minha querida orientadora a Professora Regina Rossetti da USCS, por ter acreditado na minha pessoa logo no dia da entrevista pessoal, bem como por ter confiado no meu trabalho durante o transcorrer do curso, como pela enorme paciência que demonstrou ter comigo, incluindo também as várias assessorias prestadas pela docente, concernentes a elaboração deste exaustivo trabalho acadêmico.

Com relação a escolha do Programa de Mestrado em Comunicação, este aconteceu em virtude principalmente da linha de pesquisa oferecida pela Instituição, que despertou meu interesse logo de plano, mas confesso que houve sim um empurrão de minha esposa, a fim de que realmente efetivasse mais essa conquista acadêmica na minha vida pessoal.

Meus agradecimentos se estendem também aos demais docentes, na qual tive estreito contato nas aulas e seminários, incluindo os profissionais dessa respeitada Universidade, que estiveram e participaram ativamente comigo durante minha jornada de aulas, trabalhos, orientações e demais compromissos escolares.

Por fim, menciono que cursar o PPGCOM realmente foi um grande diferencial no meu dia a dia de trabalho, inclusive sendo até perceptível pelo senso crítico e capacidade argumentativa desenvolvidos durante o curso e que agregou sensivelmente na análise de conteúdo referente a minha área de atuação na PMESP, sendo até tópico de elogios e comentários por parte de meus superiores hierárquicos.

RESUMO

A Cidadania Digital na Prevenção do *Ciberbullying* possui o objetivo principal de desenvolver boas práticas no uso das plataformas de tecnologias da informação e comunicação (TIC) e assim possibilitar a identificação e prevenção da prática do *Ciberbullying,* bem como da elaboração de um Folheto Digital que trará subsídios suficientes para a compreensão dessa problemática moderna que denota entendimento de fato *saber/conhecer* e mensurar os riscos do uso frequente da rede de *internet* pelo público jovem, situado na faixa de 12 a 18 anos de idade, bem como saber que de virtual não há absolutamente nada, pois esses ambientes funcionam em tempos reais combinando e integrando elementos, informações, dados e visualizações como a transmissão do que acontece no mundo fático, por meio do uso de uma câmera, por exemplo. O Marco Civil da *Internet* (MCI), Lei nº 12.965/2020, em seu artigo 26, destacou o dever constitucional do Estado Brasileiro em promover a Cidadania/Educação Digital como um conjunto de metodologias que refletem ensino e aprendizagem, com o notório objetivo de transmitir conhecimentos éticos, morais e de cidadania às pessoas, para a utilização e acesso em plataformas tecnológicas digitais, *internet*, aplicativos, programas e demais sistemas informatizados, respeitando sempre a dignidade da pessoa humana e o bem comum. Os crimes cibernéticos em especial o *Ciberbullying* se mostra uma problemática presente na sociedade contemporânea mundial, principalmente em épocas de pandemia da Covid-19, ocorrida no ano de 2020, pois a vítima tem sua honra, dignidade humana, liberdade de expressão, intimidade, imagem, privacidade e outros afrontados, bens jurídicos valiosos que são devidamente protegidos por disposições constitucionais vigentes no Brasil. Essas intolerâncias, por parte desses indivíduos agressores tornam para a potencial vítima do *bullie,* simplesmente impossível de conviver de maneira favorável e harmoniosa na sociedade, trazendo ainda consequências e danos desde aspectos psicológicos do indivíduo até sinais claros de baixa autoestima, com desenvolvimento inclusive de problemas patológicos, essa categoria de público, vítima do *Ciberbullying* manifesta temor de se expressar publicamente, possuem fobia social, quadros depressivos, evitam o contato com pessoas e principalmente necessitam da atenção de profissionais experientes e especialistas de algumas áreas. A Privacidade de Dados Pessoais, tratada pela Lei Geral de Proteção de Dados (LGPD) nº 13.709/18, que se espelhou no Regulamento Geral de Proteção de Dados europeu, possui seus alicerces calcados nos direitos fundamentais da privacidade, liberdade, livre iniciativa, desenvolvimento tecnológico e econômico do Brasil o que traz proteção, transparência e regulamentação acerca de dados pessoais dos cidadãos no país, abrangendo os âmbitos particulares e públicos. Ainda, os resultados apontam para um dever estatal de disseminação de uma Cidadania e Educação Digital no seio escolar com uma finalidade social, como uma matéria escolar de cunho interdisciplinar, a LGPD e o MCI mencionam que o jovem ao acessar a *internet,* busca a informação e o conhecimento, com isso exerce a cidadania e ainda essas legislações proporcionam a inclusão digital desse público. Com relação ao produto final da dissertação foi utilizado o método conhecido por *Design Thinking* na elaboração de um Folheto Digital com o escopo de identificar e prevenir a conduta do *Ciberbullying.*

Palavras-chave: Cidadania Digital; Educação Digital; Proteção e Privacidade de Dados; *Ciberbullying*; Comunicação de Interesse Público.

ABSTRACT

Digital Citizenship in the Prevention of Cyberbullying has the main objective of developing good practices in the use of information and communication technologies (ICT) platforms and thus enabling the identification and prevention of the practice of Cyberbullying, as well as the elaboration of a Digital Brochure that will bring sufficient subsidies for the understanding of this modern problem that denotes an understanding of actually knowing / knowing and measuring the risks of frequent use of the internet network by the young public, aged between 12 and 18 years old, as well as knowing that there is no virtual absolutely nothing, as these environments work in real time combining and integrating elements, information, data and visualizations as the transmission of what happens in the factual world, through the use of a camera, for example. The Civil Marco da Internet (MCI), Law nº 12.965 / 2020, in its article 26, highlighted the constitutional duty of the Brazilian State to promote Citizenship / Digital Education as a set of methodologies that reflect teaching and learning, with the notorious objective of transmitting ethical, moral and citizenship knowledge to people, for use and access in digital technological platforms, internet, applications, programs and other computerized systems, always respecting the dignity of the human person and the common good. Cyber crimes, especially cyberbullying, is a problem present in contemporary world society, especially during the Covid-19 pandemic times, which occurred in 2020, as the victim has his honor, human dignity, freedom of expression, intimacy, image , privacy and other affronts, valuable legal assets that are duly protected by constitutional provisions in force in Brazil. These intolerances, on the part of these aggressor individuals, make it possible for the potential victim of the bullie, simply impossible to live in a favorable and harmonious way in society, also bringing consequences and damages from psychological aspects of the individual to clear signs of low self-esteem, with development even of problems pathological, this category of public, victim of cyberbullying, expresses fear of expressing itself publicly, has social phobia, depressive conditions, avoids contact with people and mainly needs the attention of experienced professionals and specialists in some areas. The Privacy of Personal Data, treated by the General Data Protection Law (LGPD) No. 13.709 / 18, which was mirrored in the European General Data Protection Regulation, has its foundations based on the fundamental rights of privacy, freedom, free initiative, development technological and economic aspects of Brazil, which brings protection, transparency and regulation about the personal data of citizens in the country, covering the private and public spheres. Still, the results point to a state duty to disseminate Citizenship and Digital Education within the school with a social purpose, as an interdisciplinary school subject, the LGPD and the MCI mention that young people when accessing the internet, seek information and knowledge, thereby exercising citizenship and yet these laws provide for the digital inclusion of this public. Regarding the final product of the dissertation, the method known as Design Thinking was used in the elaboration of a Digital Brochure with the scope of identifying and preventing the conduct of Cyberbullying.

Keywords: Digital Citizenship; Digital Education; Data Protection and Privacy; Cyberbullying; Communication of Public Interest.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 PROPOSIÇÃO

1.1 Introdução

Esta dissertação trata do tema referente a Cidadania Digital como forma de prevenção e identificação da conduta de *Ciberbullying*. A prevenção aqui denota um entendimento no sentido de realmente *saber/conhecer* e mensurar os riscos do uso frequente da rede de *internet* pelo público jovem situado no intervalo de 12 a 18 anos de idade.

A escolha dessa categoria de pessoas ocorreu em virtude da legislação vigente não estabelecer uma coerência lógica de padronização, em virtude da definição do conceito de criança e adolescente, pois a Lei nº 8.069/90 conhecida como Estatuto da Criança e do Adolescente (ECA), no seu artigo 2.º, parágrafo único, define criança como sendo até os 12 anos de idade completos e adolescente o indivíduo que tenha entre 12 anos completos e 18 anos incompletos.

No entanto, a Lei nº 12.852/13 conhecida como o Estatuto da Juventude (EJ), trata como adolescente o ser humano que tenha a idade entre 15 e 18 anos e o jovem a pessoa entre 15 e 29 anos de idade, assim o referencial adotado neste trabalho adota o critério estabelecido segundo estabelece o ECA.

Pertinente, ainda se mostra com relação ao público alvo deste trabalho que de virtual não há absolutamente nada, pois aqui esses ambientes funcionam em tempos reais combinando e integrando elementos, informações, dados e visualizações como a transmissão do mundo fático, por meio do uso de uma câmera. Então acontecimentos via *internet* são reais, concretos e factuais, logo as interações existentes entre as empresas, pessoas, contendo dados e informações são exatamente as mesmas que estão fora dela, contudo, os comportamentos externos a rede está em perfeita sintonia com os intrínsecos a *internet* (CERT, 2012).

Assim os riscos, as oportunidades, as angústias, as aventuras, os prejuízos, as desvantagens e os inconvenientes que esses indivíduos assumem ao utilizar a *internet* para participarem de jogos, nada mais é do que aqueles presentes no cotidiano da vida normal desse público. Ainda os golpes aplicados por meio da

utilização da rede são muito similares aqueles que ocorrem via telefone convencional ou mesmo por mensagens de texto, por exemplo (CERT, 2012).

Claro que muito depende da *percepção/sensibilidade* de cada pessoa, ou então, de um *entendimento/malícia*, a fim de não aceitar falsas promessas, por exemplo, que se referem a quantias astronômicas em dinheiro, oriundas de mensagens de texto ou e-mail, ou ainda que solicite o fornecimento de senhas de contas correntes, cartão de crédito e/ou outros (CERT, 2012).

Ademais *mensagens/e-mail* e outros contendo as expressões *"urgente"*, *"confidencial",* ou solicitando respostas rápidas também são enormes possibilidades de golpes, sobretudo quando há a presença de erros gramaticais e de ortografia em frases ordenadas que denotam um forte indicativo no uso de programas contendo tradutores de *texto/palavras*, que apresentam erros de tradução e concordâncias verbal e nominal (CERT, 2012).

A desconfiança sempre será um bom remédio de prevenção aos crimes cibernéticos, principalmente aqueles em que existem solicitações de realização de pagamentos com a promessa futura de receber um valor maior (CERT, 2012).

Um aspecto de relevância no cenário do *cibercrimes se trata* de situações que envolvam a compra impulsiva de mercadorias ofertadas via rede de *internet*, com o intuito de garantir um eventual preço reduzido, conhecida como "*Negócio muito Lucrativo",* aquele imperdível sem, contudo, verificar questões concernentes a pesquisas prévias, contendo opinião de outros compradores, grau de satisfação em relação a qualidade do produto adquirido e a empresa, enfim tratativas simples que estão relacionadas a cautela e precaução que a pessoa deve apresentar diante dessa situação, que muitas das vezes parece ser simples e tranquila (CERT, 2012).

A postura preventiva do indivíduo realmente ajuda a evitar a *concretude/ acontecimento* do delito virtual na vida das pessoas, basta simplesmente questionar-se, por que justamente você seria o ser contemplado com tal benesse, com infinitos usuários de *internet* no planeta, você em específico seria o escolhido, ou então, como chegaram até você para receber o suposto benefício tratado na mensagem, o que não se mostra nada oportuno e razoável (CERT, 2012).

No caso do *Ciberbullying* escopo desse trabalho, a prevenção recai em algumas atitudes louváveis e eficientes, como por exemplo, evitar ao máximo exposições desnecessárias de cunho íntimo ou não, junto as redes sociais, bem como bloquear de imediato pessoas mal-intencionadas, jamais disseminar fotos

contendo cenas de nudez parcial ou total, mesmo que se trate de parceiro, parente ou quem for, ainda que de extrema confiança.

Ainda trabalhar a tolerância (*racial, religiosa, física, social, cultural e regional*) em relação a outros jovens, a auto aceitação é importante também no processo de formação da personalidade desse adolescente, aprender a lidar com a manifestação de sentimentos e pensamentos, com o escopo de manter sempre um relacionamento saudável e harmonioso.

O jovem deve também se ater ao fato de que ao sofrer ataques perversos *on line,* estes geram sim estragos e que são reais, que representem práticas delitivas tipificadas junto ao Código Penal, portanto, são crimes que configuram afrontas contra a honra do ser humano, a injúria, a difamação e a calúnia, acompanhados na maioria das vezes do instituto de dano moral. O procedimento legal a ser observado deve ser o deslocamento até uma Delegacia de Polícia da circunscrição, na companhia dos pais ou pessoa responsável, com o intuito de registrar formalmente a ocorrência, com a adoção das demais providências legais cabíveis, no contexto de polícia judiciária.

O adolescente ou mesmo a criança ao ser vitimado por agressões virtuais deve antes de qualquer atitude conversar pessoalmente e explicar o ocorrido a seus pais ou responsável, até a uma pessoa da máxima confiança do menor, a fim de que esses indivíduos possam prestar o devido apoio familiar, psicológico e criminal, pois a vítima nesse momento se sente acuada em virtude do ambiente digital ser infinito e o mais grave, não saber como se defender e de quem.

1.2 Origem do Estudo

O gosto e interesse pela pesquisa surgiu após frequentar o Curso de Direito Digital ofertado pelo Instituto de Ensino e Pesquisa (Insper), localizado na cidade de São Paulo/SP. O presente trabalho versa como um dos temas centrais a Educação Digital associada ao uso frequente da *internet* nos dias atuais, ainda como ferramenta de trabalho, estudo, lazer e outros, assim como destacou a obra Educação Digital de Abrusio (2015, p. 22). O tema é recente e de grande repercussão como, por exemplo, os casos de massacres ocorridos na Escola Municipal Professor Raul Brasil localizada na cidade de Suzano/SP e nas mesquitas

situadas na cidade de *Christchurch*, Nova Zelândia, ambos ocorridos no ano de 2019, portanto, fatos recentes.

Após realização de pesquisas preliminares, foi verificada a existência de uma lacuna acerca da relação entre a *Internet*, a Cidadania e Educação Digital, os *Cibercrimes*, uma vez que existem pouquíssimos trabalhos sobre esse tema tão atual, relevante e preocupante socialmente. Assim, a contribuição da presente dissertação será de extrema valia para o mundo acadêmico contemporâneo.

Convém discorrer a respeito da Educação Digital, os aspectos conceituais apresentados por Fidalgo (2019), que abrange a Educação como algo ligado a ética digital, *ciber cidadania* e o respeito as demais pessoas, segundo as normas de convivência costumeiras e as legais.

O mundo digital se transforma de maneira acelerada a cada dia que passa, atingindo amplamente os membros de toda a nossa sociedade. A transmissão ao vivo do massacre em Christchurch na Nova Zelândia, via rede social *Facebook*, se assemelhou a jogos *virtuais/digitais* de combate, com a utilização de armas de fogo, demonstra que o mundo de agora está cada vez mais conectado de forma *on line* e estabelecendo comunicações instantâneas, seja em qual parte for do mundo, portanto, pouco importa a distância terrestre ou aérea, o fato é que o uso assíduo da *internet* está no dia a dia das pessoas comuns, bem como profundo e arraigado na sociedade contemporânea.

Ademais, há a necessidade de salientar sobre os valores pessoais desses indivíduos, pois funcionam como verdadeiros balizadores implícitos e indicadores próprios da pessoa humana, para a consecução das mais variadas atitudes, ações, condutas e práticas do homem médio, com o único intuito de promover boas condutas e práticas junto a rede de *internet.*

Justamente por isso, é tão essencial associar o ensino digital à questão dos valores pessoais, atualmente há uma imensidão de estímulos que recebemos no convívio diário com pessoas distintas, seja *off line* ou mesmo conectado, que na maioria das vezes são informações sem valor agregado algum, sem sentido e analisando o mérito da informação, sem a necessidade de existirem no mundo dos fatos, assim completamente desprezíveis (ABRUSIO, 2015, p. 17).

A Educação sob a ótica dos valores constrói a cidadania e a dignidade do ser humano, seja por meio do mundo *on line* ou mesmo *off line*, contudo, as liberdades devem ser ponderadas, respeitadas e analisadas com cautela, a fim de

alcançarmos a verdadeira consciência digital, enfrentando de frente a alegria e a tristeza com hombridade, energia e harmonia (ABRUSIO, 2015, p. 94).

1.3 Problematização

A problematização desta pesquisa parte da necessidade de cada vez mais se desenvolver boas práticas junto ao uso do ambiente virtual visando à segurança das tecnologias da informação e consequentemente da comunicação, bem como a proteção acerca de possíveis ameaças digitais atinentes a condutas direcionadas contra a *pessoa humana, principalmente no tocante, a sua imagem, honra, dignidade humana, liberdade de expressão, intimidade e privacidade, associadas* a dicas, cuidados, posturas comportamentais, com o intuito de aumentar a segurança dos usuários da rede mundial de *internet*, especialmente dos dados, computadores e outros dispositivos móveis utilizados no dia a dia dos indivíduos.

No transcorrer deste estudo, as Tecnologias da Informação e da Comunicação serão tratadas com as siglas TIC, que na verdade são entendidas como um aglomerado de recursos de tecnologia muito utilizados meio cibernético e de forma integrada para a troca eficiente de informações, experiências e comunicações, ofertando ao público jovem a inclusão digital e a democratização das redes, grupos e fóruns.

Esta pesquisa pretende responder a seguinte pergunta problema:

Como a Cidadania Digital pode contribuir para o desenvolvimento de boas práticas aliadas a medidas técnicas, no uso das plataformas de tecnologias da informação e comunicação (TIC), a fim de identificar e prevenir o *Ciberbullying*?

1.4 Objetivos

Objetivo principal

Contribuir para o desenvolvimento de boas práticas no uso das plataformas digitais (TIC), a fim de identificar e prevenir a prática do *Ciberbullying*, por meio do instituto da Cidadania Digital.

Objetivo secundário

Propor um folheto digital com foco no público alvo, ou seja, jovens e adolescentes com idades entre 12 a 18 anos de idade, acerca das tratativas de identificação e prevenção do delito de *Ciberbullying*.

1.5 Proposta de Intervenção

O folheto digital proposto se resume a um material de comunicação de ordem prática, eficiente e com uma leitura *rápida/dinâmica*, que proporciona um entendimento sobre essa problemática tão presente de *Ciberbullying,* muito comum atualmente no mundo contemporâneo.

É uma ferramenta de marketing direcionada a publicidade educacional e de cidadania, pois apresenta um conteúdo bem direcionado, na qual a pessoa que lê, pode ou não se identificar com a conduta ofensiva descrita e saber que aquilo que está sofrendo se trata de um constrangimento, que na verdade é nocivo e necessita de ajuda de pessoas confiáveis.

1.6 Justificativa da Pesquisa

A necessidade da compreensão dos acontecimentos atuais envolvendo o cenário virtual tanto no Brasil como no mundo são perquirições imediatas. A Cidadania Digital se mostra fundamental para disseminação de um papel contendo normas e regras sociais, bom senso e respeito digital que sustentarão um bom convívio e relacionamento entre pessoas, bem como para uma prevenção do *Ciberbullying,* pois as novas tecnologias da informação e da comunicação requerem novas metodologias de educação, investigação e combate a este ilícito virtual pernicioso.

O pensamento crítico do indivíduo no contexto digital e possuidor de hábitos adequados, bem como de suas crenças colocadas em prática no dia a dia, proporcionará o crescimento do indivíduo em sua plenitude como ser humano, que se tornará uma característica contínua e eficaz, de maneira que caminhará sempre na direção da *pedra de toque*, que se chama Cidadania Digital e que no fundo, será utilizada como uma ferramenta fundamental, para a construção de um processo de

ensino sistemático, uma aprendizagem virtual das pessoas no mundo e a formação de uma sociedade pautada no bem estar social, no respeito, na ética e moral.

A Cidadania Digital busca inegavelmente o instituto da segurança da informação, nesse cenário tecnológico comunicacional atual, por isso estão umbilicalmente ligados e com isso as próprias tecnologias da informação e comunicação estarão ainda mais disponíveis no cotidiano dos indivíduos, trazendo como grande segredo a utilização das plataformas virtuais com sabedoria, respeito, empatia, cidadania e acima de tudo dignidade como atributo essencial da pessoa humana. Assim uma formação educacional consistente contribuirá consideravelmente no uso regular da rede de *internet.*

As culturas e interações entre os agentes públicos e atores sociais (governo, Estado, sociedade civil, inclusive partidos políticos, empresas, terceiro setor e cada indivíduo como pessoa humana) atravessa os diversos ambientes da comunicação e informação, pois estão envolvidos diretamente com o interesse público, com o intuito da busca do essencial compromisso do diálogo social, respeitando as diferenças raciais, culturais, étnicas, religiosas, de opinião e partidárias (ideológicas) chegará com certeza a processos sistemáticos de consensos e com isso se fortalecerá a consolidação da democracia na vida dos cidadãos (DUARTE, 2007).

1.7 Metodologia

As atividades serão basicamente de pesquisa, combinadas com o estudo direcionado ao tema, por meio de uma abordagem qualitativa, tipo exploratória, com uma revisão bibliográfica e documental, bem como a análise de leis vigentes no ordenamento jurídico pátrio aliadas à seleção, acompanhamento, descrição e análise de alguns casos pontuais que possuem elementos relevantes para esse trabalho acadêmico e científico, assim os desdobramentos da utilização da rede de *internet* para a consecução e consumação do *Ciberbullying* via rede mundial de computadores no Brasil e no mundo.

1.8 Delimitação do Estudo

A Cidadania Digital associada ao uso frequente da *internet* como ferramenta necessária de trabalho, estudo, lazer e outras necessidades imbuídas atualmente no

cotidiano das pessoas humanas. Assim é relevante estudar essas relações entre as temáticas *Internet*, Cidadania Digital, Proteção e Privacidade de Dados, Educação Digital e o *Ciberbullying*, uma vez que este trabalho versa sobre um assunto tão atual e preocupante socialmente, pois em época de pandemia da Covid-19 a abordagem desse delito cibernético ocorrido no Brasil e ao redor do mundo se mostra oportuna e conveniente em virtude principalmente das regras sanitárias de isolamento e confinamento social.

Trazendo o cenário da comunicação digital via *internet*, segundo entendimento de Levy (1999), filósofo francês radicado no Canadá, aborda que atualmente, e calcada nas imensas interconexões mundiais ou mesmo locais, de computadores, telefones celulares e outros aparelhos ou mesmo dispositivos com a rede de *internet*, ocorre a significativa inclusão dos institutos da inteligência artificial e *internet* das coisas em suas discussões.

Com certeza propicia, o indiscutível mergulho nas relações contemporâneas de comunicação e informação humana aliado a efetiva produção de conhecimento e associado a bela abordagem sobre a figura do professor em seu papel central no sistema educacional, para que atue como um verdadeiro incentivador de aspectos relacionados a questões de inteligência coletiva, como também um fomentador de relevantes informações consubstanciadas na construção efetiva do conhecimento, desenvolvimento intelectual de seus alunos e a contributiva formação do senso crítico (LEVY, 1999).

Por sua vez, o sociólogo espanhol Castells (2013) afirma que a comunicação digital no contexto moderno se mostra uma nova estrutura socialmente constituída, consubstanciando em uma sociedade dispostas em rede. Assim a comunicação atua com o recebimento de uma diversidade de fontes e através dessas interações se consolidará as necessárias alterações sociais.

Com isso a *internet* é hoje tão importante quanto a televisão foi em tempos passados e cabe lembrar ainda que vivemos cercados de uma comunicação tipicamente híbrida, ou seja, oriunda de meios comunicativos de diferentes origens e dessa maneira a troca de informações são frequentes, oportunas e convenientes, por isso a relevância no estabelecimento desses meios de comunicação, pois de fato as relações de poder da sociedade civil, instituições e figuras políticas sofrem influências das mais variadas possíveis, portanto, o poder da comunicação digital é fruto de uma sociedade disposta atualmente pela rede de *internet*.

As alterações das mídias com o sinal dos tempos, sejam de vinil para MP3, por exemplo, nunca se esvaíram, pois simplesmente se renovaram nos anos que se passaram, sejam em aspectos relacionados a modernidade, mas que o intuito final sempre será o da satisfação do público em geral, de consumidores da informação advindas de meios de comunicação diversos e distintos, sejam antigos ou não (JENKINS, 2015).

1.9 Vinculação à área de Concentração e à Linha de Pesquisa do Programa

A temática da Cidadania Digital na prevenção de crimes digitais está intrinsicamente relacionada com a comunicação de interesse público, por meio da Teoria do Interesse Comum.

Hoje a *internet* também se mostra um espaço denominado como praça pública. O ciberespaço público atual é conhecido pela maioria dos seres humanos, por possuir as mesmas características da antiga e convencional praça pública (praça com a tradicional igreja católica no centro da pequena cidade de interior), fazendo com que o internauta exerça o atuante papel de sujeito e com isso haja uma efetiva participação junto ao processo de diálogo, argumentação e discurso na busca incessante do consenso, alavancando a consolidação da democracia no meio social (DUARTE, 2007).

Portanto, a esfera pública é um espaço comum a todos, ou seja, que está à disposição das pessoas, por uma variedade de meios, oportuno mencionar as redes tecnologicamente mediadas ou mesmo a tradicional conversa pessoal frente a frente, com o intuito de discussão, argumentação e consenso, obtido por um sistema demasiadamente conhecido pela troca de ideias, informações e dados (TAYLOR, 2010).

O bem comum aqui neste estudo será tratado sob a ótica do interesse público, portanto, a palavra *“comum”* significa a raiz da comunicação, sendo que o *objetivo/finalidade/escopo* a serem perseguidos pelos usuários da rede de *internet*, será a propagação na sociedade em geral de bons hábitos digitais, segundo os ditames do instituto da Cidadania Digital, aliado a utilização da rede de *internet* com consciência, segurança, paciência e sem ansiedades, ou seja, moderadamente e de forma palpável, pois, do outro lado do computador, *tablet, smartphone* ou mesmo do

aparelho celular, existem outros seres humanos, que possuem os mesmos sentimentos, temores e anseios (MARTINS FILHO, 2000).

Contudo, a comunicação de interesse público, ultrapassa a necessária comunicação pública (incluindo aqui o grande hemisfério estatal dos governos e Estados, como a sociedade civil e seus partidos políticos, empresas, terceiro setor e cada indivíduo como pessoa humana), pois os reais beneficiários serão sempre os componentes da sociedade em geral, portanto, o trabalho busca o escopo do interesse público (DUARTE, 2007).

A comunicação pública se difere da comunicação política, na qual os discursos se referem as ações específicas de governos, partidos e seus respectivos agentes na conquista da opinião pública em questões afetas a ideias ou atividades que tenham relação com o poder político, seja em épocas de eleições ou não (DUARTE, 2007).

Por fim, a transparência das informações versa sobre o compromisso de uma atuação *eficiente/transparente/responsável* concernente a assuntos públicos, o que denota o tratamento de informações, a prestação de contas, a fiscalização e o fomento de acesso pelo cidadão aos serviços públicos oferecidos. Em outro patamar o acesso está calcado na facilidade do indivíduo em conseguir as informações que procura junto ao órgão público específico, opinar a respeito da prestação, acompanhar a gestão pública e com isso ter uma maior *proximidade/atratividade* com a coisa pública (DUARTE, 2007).

2 REFERENCIAL CONCEITUAL

Esta seção apresenta os conceitos que serão utilizados ao longo do desenvolvimento dessa importante pesquisa e servirão para fundamentar a proposta de intervenção. Primeiramente abordando o aspecto da Cidadania e Educação Digital, que tratam do cenário relacionado à cidadania, respeito e dignidade humana da pessoa, depois a questão crucial do crime cibernético do *Ciberbullying* que afetam frontalmente os bens jurídicos tutelados pela legislação penal brasileira e outras, ao final, a privacidade de dados, que regulamenta, o uso, proteção e a transparência para o tratamento de dados pessoais dos jovens no Brasil, seja em âmbito público ou particular e ainda de modo *on line* ou mesmo *off line*.

No aspecto da comunicação midiática e de *internet*, o americano e professor de Ciências Humanas, Jenkins (2015) ressalta que pessoas são incentivadas a buscar constantemente informações em meios de comunicação distintos e por isso os emissores de conteúdo devem repensar suas maneiras de oferecer conteúdo o que exprime seu pensamento de *cultura de convergência*, pois segundo o estudioso há um forte entrelaçamento das mídias antigas e atuais.

Em decorrência lógica Jenkins (2015) trata de uma transformação concernente aos aspectos de produção e consumo dos meios de comunicação TIC existentes hoje no contexto contemporâneo.

Com o progresso tecnológico as TIC são atualmente um instrumento importante e necessário na comunicação, informação e desenvolvimento humano, envolvendo som, imagem, movimento e com uma abrangência em diversos setores da vida social.

2.1 Cidadania Digital

A conectividade atualmente é parte integrante das variadas rotinas do dia a dia dos indivíduos, levando em conta é claro aspectos da efetiva existência da rede de *internet*, nos quatro cantos do globo terrestre, contudo, há a necessidade da utilização da *internet* aliada a normas, bem como em obediência a aspectos éticos, morais, do uso consciente dos recursos tecnológicos disponibilizados e do usufruto consciente de todos esses benefícios, por isso dá pertinência e relevância do instituto da cidadania digital. O ligeiro crescimento das tecnologias da informação e

comunicação trouxeram uma alavancagem de benefícios a sociedade moderna (SANTIAGO, 2019).

Trata-se de um conceito que traça delineamentos baseados no fomento a consciência humana, de que os recursos disponibilizados para as pessoas exigem sim uma adoção firme de condutas amparadas em direitos e deveres, portanto, vislumbra-se ações positivas. Assim são pressupostos presentes em países *alicerçados/fundados* em regimes democráticos (SANTIAGO, 2019).

Claro que essa seara dos direitos e deveres, que na verdade são originados segundo a Constituição Federal de cada país, concernentes a um mundo virtual, assumes sentidos distintos da realidade fática, tendo em vista o aspecto essencial dessa abrangência da realidade fictícia *on line* ser infinitamente superior (SANTIAGO, 2019).

O uso de recursos tecnológicos como a rede de *internet* pelos indivíduos, requer ações sistêmicas fundamentais, no tocante ao comportamento e ações de cada pessoa, pois a cada dia que passa a sociedade almeja o uso mais responsável desses recursos colocados a propensão dos seres humanos (SANTIAGO, 2019).

Por isso, que a cidadania digital se mostra um importante elemento no relevo atual e ainda se sacramente como um direito fundamental dos cidadãos de bem, implementando o respeito aos valores éticos que delineiem a liberdade digital pleiteada, para que essa utilização da rede represente honestos benefícios aliados a uma efetiva segurança digital (SANTIAGO, 2019).

Abordar a cidadania digital é atitude indispensável para uma boa compreensão e fomento do uso responsável da *internet*. O instituto está intrinsicamente relacionado a diversos cenários que envolvem e dinamizam contextos cibernéticos (SANTIAGO, 2019).

Como *alcance/cobertura/amplitude* em assuntos valorosos como educação, segurança, privacidade, *e-commerce*, comunicação, certificação digital, legislação na rede, nível de alfabetização, empreendedorismo, responsabilidade social dentre outros (SANTIAGO, 2019).

Inclusive o conceito da cidadania digital abarca com certeza princípios, valores e *ações/condutas* que refletem em uma civilidade acentuada, que focam diretamente no ingresso consciente das pessoas a rede de serviços tecnologicamente mediada. Dessa forma há a necessidade de educar os usuários, a

fim de promoção de uma responsabilidade perene, do respeito recíproco, para se utilizar dos prazeres que a rede proporciona (SANTIAGO, 2019).

Essa transformação digital está pautada na era contemporânea, pois o aspecto social não trata apenas de seres humanos, mas hoje inclusive sim de algoritmos, *big data* e inteligências artificiais dentre outros, portanto, há uma grande interação com as redes digitais, fluxos de dados e tecnologias inteligentes (DI FELICE *et al*., 2018).

As formas não humanas de inteligência possibilitam a interação entre pessoas e dados, por meio da participação nas redes e propiciando um efetivo diálogo e estendendo essa relação dos *bits* e *bytes*, para além de espaços físicos conhecidos (DI FELICE *et al*., 2018).

Mas as redes de dados e links, por exemplo, exigem o conhecimento das pessoas, por isso que a promoção do exercício de regulamentos, obrigações, deveres e direitos são necessários. Os *softwares*, regras, algoritmos devem estar estruturados em garantia aos direitos dos indivíduos (DI FELICE *et al*., 2018).

O comportamento *on line* ético, probo, reflete em incumbências oriundas da família, dos professores, logo do Estado, contudo, as crianças e adolescentes poderão *entender/aprender* a exata necessidade desse instituto que não apenas retrata atenção a uma educação formal, mais do que isso se trata de simplesmente de uma função social de tratativas sobre a construção de um futuro promissor enveredado em valores, ensinamentos e ações (SANTIAGO, 2019).

O escopo sem dúvidas é de prepará-las para um cenário futurístico recheado de tecnologias e ao mesmo tempo proporcionar que possam desfrutar de seus benefícios, vantagens, oportunidades e conhecer as reais ameaças contidas nesse ambiente midiático contemporâneo, bem como de lidar com esse *progresso/prosperidade* sem *tolher/ofender/invadir* o espaço do outro, interferindo principalmente em seus direitos e deveres (SANTIAGO, 2019).

Portanto, existem limites a serem seguidos, respeitando sempre é claro as devidas proporções da ética, moral e da legislação em vigor, que certamente determinará um uso adequado e civilizado na busca das vantagens que a tecnologia proporciona ao cidadão (SANTIAGO, 2019).

A cidadania digital ainda reflete traços na área pedagógica, sob um aspecto multidisciplinar, por isso que a educação exerce um papel de metamorfose no viés

da utilização da rede alinhado aos princípios relativos dos direitos humanos nas diferentes esferas da sociedade humana (SANTIAGO, 2019).

Obviamente que a aplicação dos princípios norteadores do instituto da cidadania digital não versa apenas sobre o uso da *internet*, mais do que isso claro, pois sustenta, garante, afiança a responsabilidade do usuário em relação a todos os recursos tecnológicos colocados à disposição dos indivíduos (SANTIAGO, 2019).

As pessoas com certeza atingirão um patamar de cidadãos digitais na oportunidade em que conseguirem aliar a fruição de seus direitos consagrados constitucionalmente e em sua plenitude com o fiel cumprimento de seus deveres oriundos das plataformas digitais oriundas de um ambiente digital (SANTIAGO, 2019).

A legalidade das condutas pessoais no ambiente virtual também alia reflexões como a exposição demasiada de materiais e conteúdos íntimos consensuais ou não, por exemplo, o que fere com certeza cenários de segurança e privacidade, contribuindo para a destruição da boa fama e reputação da pessoa humana (SANTIAGO, 2019).

A sociedade atual possui o dever de educar para uma cidadania digital, abrangendo os estabelecimentos de ensinos públicos e privados, estabelecendo interações saudáveis e responsáveis entre pessoas e formas não humanas de conectividades (DI FELICE *et al*., 2018).

As tratativas relacionadas ao instituto da cidadania digital, já se encontram integradas nas distintas formas do uso ético, moral e eficiente das tecnologias da informação colocadas à disposição das pessoas. As maneiras de proteção da rotina virtual devem ser acompanhadas de inovações que aconteceram também do mundo dos fatos em relação à segurança. No final das contas, todos os indivíduos ainda estão expostos a riscos de alguma maneira, seja na rede de *internet* ou mesmo na vivência da realidade.

2.1.1 Educação Digital

No mundo das tecnologias da informação e da comunicação, o instituto da Educação Digital não versa apenas sobre conceitos voltados exclusivamente a ensinamentos de pessoas, a fim de que elas realizem apenas e efetivamente trocas de mensagens eletrônicas como acontecem em *e-mail, Whatsapp, Telegram,*

Instagram, Facebook e outras plataformas digitais existentes no mundo atual e inseridas no dia a dia dos indivíduos, que inclusive as utilizam como uma ferramenta indispensável para a consecução de seus trabalhos ou estudos habituais.

Desenvolver a tão sonhada Educação Digital é uma tarefa árdua, estratégica e difícil que visa inclusive um futuro promissor aos países, como também pelo importante papel junto ao desenvolvimento econômico e social do Brasil, bem como pela relevância no cenário da segurança nacional, da informação, consequentemente refletindo no aspecto da ordem pública como segurança pública (MIRONOVA *et al*, 2019).

Assim o cerne da Educação Digital abarca um consagrado cenário, ainda maior, no aspecto de uma possível remodelação de currículos escolares, com o intuito de propiciar uma adequação às novas formas de trabalho existentes, estudo, vida e convivência diária entre os seres humanos. Por isso, que há necessidade eminente de trazer a Educação Digital para um patamar idêntico ou superior às outras matérias ensinadas em ambiente escolar, seja em estabelecimento público ou privado, invocando para isso, se necessitar até os aspectos da interdisciplinaridade disponibilizados junto ao ensino brasileiro.

A Educação Digital refere-se ao uso das tecnologias e dos recursos educacionais disponibilizados com o objetivo de preparar as pessoas para uma vida junto à sociedade da informação, pois o regresso tecnológico é impossível, ou seja, existe a necessidade da real inclusão social desses indivíduos no mundo cibernético, assegurando-lhes a sociabilidade necessária, a cultura e a aprendizagem digital (ABRUSIO, 2015, p. 186).

O filósofo, sociólogo e pesquisador Levy (1999) denota que os modelos atuais de ensino fundamentados na tradição são questionáveis a luz da atualidade, em virtude das inúmeras inovações tecnológicas existentes e colocadas em uso dia após dia, que afetam inclusive as relações de trabalho existentes, geram novos e amplos conhecimentos aliados a transmissão de ideias e saberes. O ciberespaço, por exemplo, apresenta alterações de funções cognitivas humanas, por meio da combinação de variados dispositivos de comunicação eletrônicos na transmissão de informações e dados.

Jenkins (2015), por sua vez defende a inclusão de pessoas na cultura participativa ao mencionar que a ausência de uma educação significativa no acesso à rede de comunidades, isso com o escopo da busca do conhecimento e

informação, proporciona a efetividade das relações ativas e construtivas permitidas pelas mídias.

Portanto, a Educação Digital, não se mostra uma opção, mas uma realidade essencial junto ao contexto da aprendizagem, seja escolar, de trabalho, mesmo de lazer, enfim, representa a efetividade da integração das pessoas ao mundo e do mundo para as pessoas, como ele realmente é e está, conhecer a concretude de suas ameaças digitais, suas potencialidades de riscos, inclusive por meio das várias práticas criminosas existentes hoje, entender os desafios apresentados, avaliar as oportunidades, enfim o cerne da discussão é propiciar as pessoas a construção de uma sociedade mais coesa, firme e preparada para suportar as novidades que estão aqui diante de nós e que outras mais aparecerão com toda a certeza, por isso da necessidade das aquisições de habilidades pessoais e das necessárias contribuições efetivas, para o mundo com a experiência adquirida no contexto virtual.

A Educação Digital auxilia na conscientização do uso da tecnologia virtual para que o internauta interaja na rede mundial de computadores de forma ética, correta, sem amarras, livre de ameaças e riscos, ou que estes sejam minimizados demasiadamente, evitando-se práticas criminosas a todo custo (ABRUSIO, 2015, p. 186).

O Marco Civil da *Internet*, descrito por meio da Lei nº 12.965, de 23 de abril de 2014, em seu artigo 26, menciona que:

> o cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da *internet* como ferramenta como exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico (BRASIL, 2014).

O instituto da Educação Digital por sua vez não se confunde com a educação na seara visando o ensino da informática em escolas, uma vez que são aspectos completamente distintos, a primeira se preocupa em formar cidadãos conscientes das características da vida na rede de *internet,* seus riscos, direitos, obrigações, limites e possibilidades, ao passo que a segunda se refere apenas ao uso da informática como uma simples ferramenta inserida em uma matéria escolar, portanto, são conceitos com anos luz de diferença (ABRUSIO, 2015, p. 186).

Nesse contexto, a Educação Digital é o conjunto de metodologias que refletem ensino e aprendizagem, com o notório objetivo de transmitir conhecimentos éticos e de cidadania, para o uso e acesso em plataformas tecnológicas digitais, *internet*, nos aplicativos, programas e demais sistemas informatizados, respeitando-se a dignidade da pessoa humana e o bem comum como interesse público (FIDALGO, 2019).

O bem comum será tratado sob o prisma do interesse público, como um norte a ser atingido, perseguido, assim, o escopo no qual a Educação Digital buscará sempre será a propagação para a sociedade de bons hábitos cibernéticos, bem como utilizar a rede de *internet* com consciência, segurança, paciência e sem ansiedades, moderadamente e de forma palpável, pois, do outro lado do computador, *tablet, smartphone* ou mesmo do aparelho celular, estão outros seres humanos que possuem os mesmos sentimentos, assim como no mundo real, com possibilidades concretas de proporcionar maldades inclusive. Por isso, a importância em não compartilhar dados pessoais ou bancários com pessoas estranhas, evitar postagens desnecessárias em sites e redes sociais e que não tragam a construção de saberes, são atitudes muito bem-vindas nesse contexto cibernético atual e avançado.

Assim, o pensamento crítico digital do indivíduo, com esses hábitos e crenças colocados em prática no dia a dia proporcionará o crescimento do indivíduo em sua plenitude como ser humano, que se tornará uma característica contínua e eficaz, de maneira que caminhará sempre na direção da *pedra de toque*, que se chama Educação Digital e, que no fundo, será utilizada como uma ferramenta fundamental para a construção do processo de ensino e aprendizagem virtual das pessoas no mundo.

Portanto, a Educação Digital busca inegavelmente o instituto da segurança da informação nesse contexto tecnológico atual, assim estão umbilicalmente ligados e com isso as próprias tecnologias da informação estarão ainda mais disponíveis no cotidiano dos indivíduos, trazendo como grande segredo a utilização com sabedoria, respeito, empatia, cidadania e acima de tudo dignidade como atributo essencial da pessoa humana.

2.1.2 Literacia Informacional das Mídias

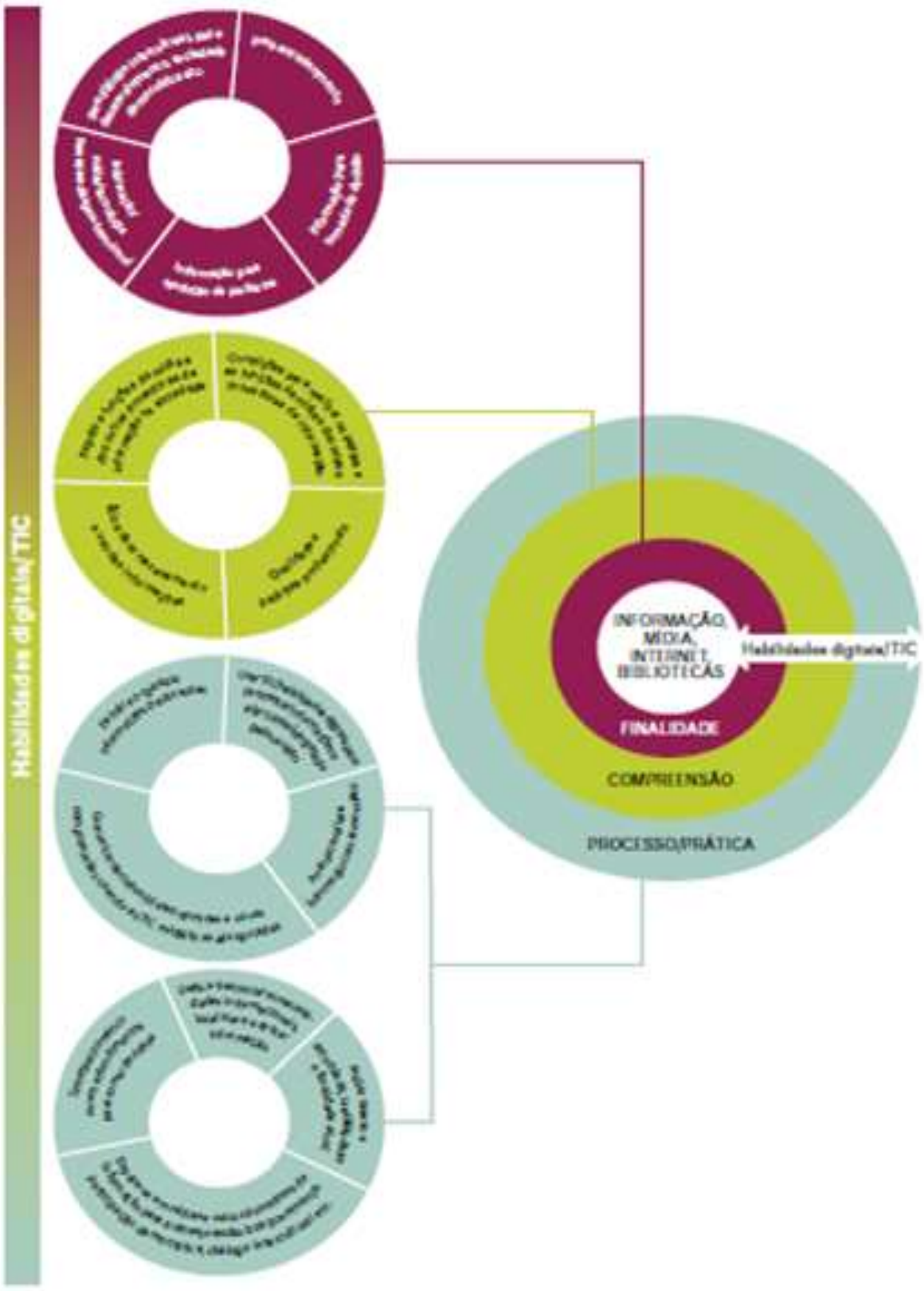
No mundo contemporâneo norteado pelas TIC, o público jovem certamente está cercado, como também farto de mídias, a fim de poderem exercer a garantia constitucional da liberdade de expressão e pensamento, mas em contrapartida há questões pertinentes e referentes a segurança em ambiente cibernético, incluindo a privacidade e integridade da pessoa humana, principalmente dos menores que devem ser observadas, as TIC, contudo, não se restringem a rede e abrangem outros provedores de informação, como editoras, museus, acervos, bibliotecas, rádios, TV e os dispositivos móveis (UNESCO, 2016).

A alfabetização no acesso regular da *internet*, sendo a digital e das mídias sociais, todas essas maneiras de alfabetizações são relevantes nesse contexto que envolve o *Ciberbullying,* assim as estratégias contidas no instituto da Cidadania Digital proporcionam o conhecimento de maneira que esse público possa se inserir de maneira democrática e responsável no mundo digital contemporâneo e que o regresso já não é mais possível.

Com certeza a presença da Cidadania Digital permitirá que os jovens adquiram os meios necessários, a fim de se protegerem de possíveis ameaças as suas liberdades de expressão, auto expressão e determinação, bem como de uma efetiva participação democrática na sociedade moderna, munidos de um afinado senso crítico que estará adequado obviamente a idade desses jovens.

Assim a figura abaixo agrega conhecimento, pois demonstra as habilidades digitais/TIC, a alfabetização midiática e informacional, bem como o meio nas quais ocorre a comunicação e transmissão da informação.

Figura 1 - Alfabetização Midiática e Informacional: Uma Proposta de Matriz Conceitual



Fonte: UNESCO (2016).

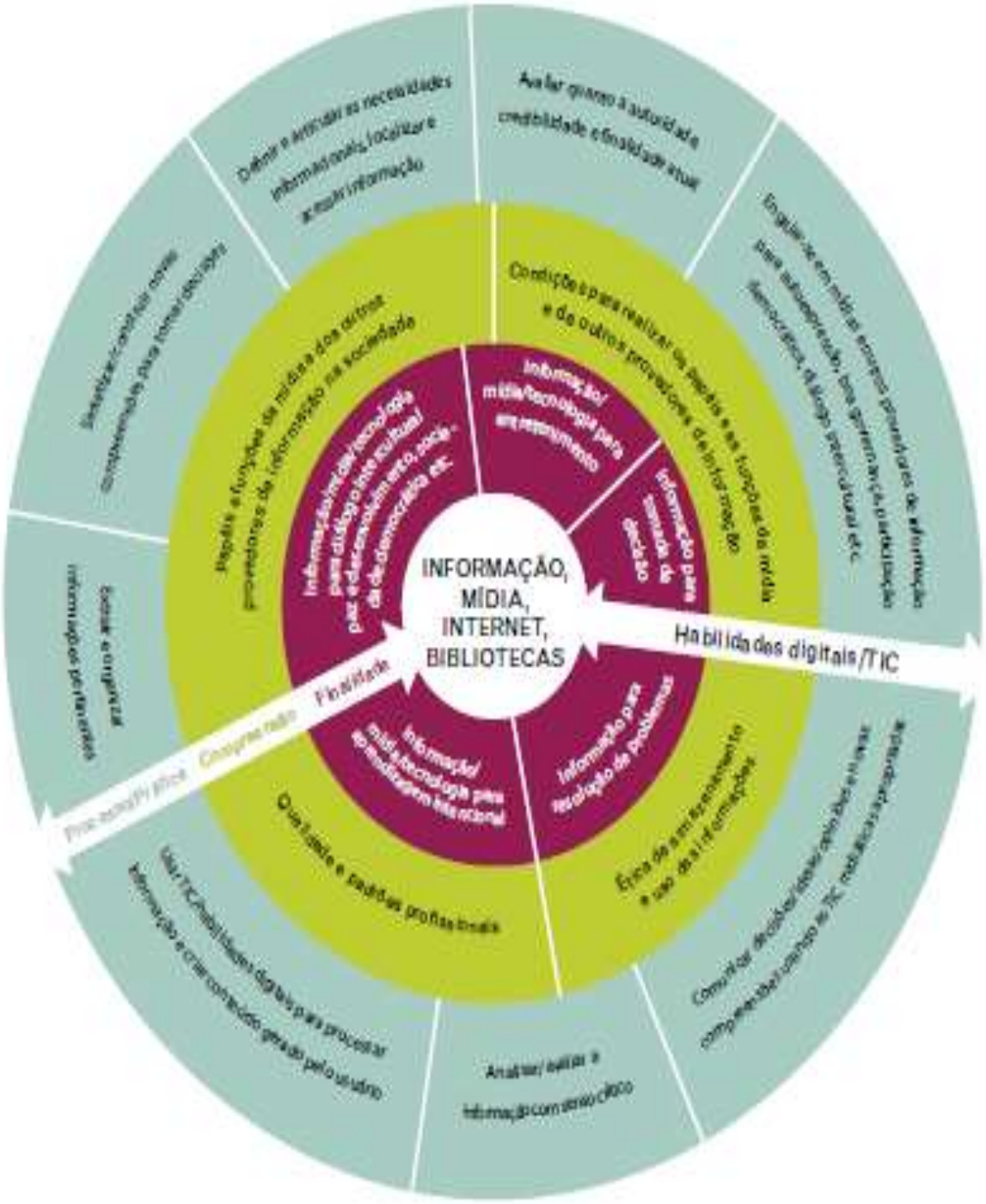
A literacia informacional desenvolve um direcionamento do público jovem que está relacionado a um consumo midiático, por exemplo, apresentando o conteúdo de uma gama maior de interatividades, como acontece atualmente com o efeito *YouTubers*, que consumidores fiéis atuam em sua produção, portanto, são pessoas produtoras de materiais que são consumidos por inúmeros indivíduos hoje no mundo civilizado (TOALDO; MARQUES; LIMA, 2017).

Assim existem vários materiais que estão direcionados a esse público adolescente, que consequentemente abrigam novas descrições comunicacionais que nasceram com essas novas mídias.

Portanto, a literacia informacional se tornou fundamental na elaboração e na constância das relações sociais em rede, esta palavra *"literacia"* está demasiadamente disseminada no Brasil como sendo uma forma de *alfabetização humana*, assim os sujeitos desenvolvem condições técnicas para uma percepção, entendimento e manifestação a viáveis construções, obviamente que por meio de um desenvolvimento de informações (TONDO, 2019).

A figura abaixo menciona alguns aspectos relevantes como as instituições da informação (como acontece a comunicação), a finalidade, compreensão, o processo e prática, a fim de fazer um uso ético da informação, mídia e das plataformas TIC, aliada a garantia de acesso a informação, por meio do uso da *internet* como meio e fim do exercício da cidadania.

Figura 2 - Proposta de Matriz Conceitual



Fonte: UNESCO (2016).

Com relação a matriz acima, a figura traz algumas maneiras de como a informação é disseminada e ainda *trata/enxerga* a mídia como uma instituição, no tocante, a rádios, TV e dispositivos móveis, por exemplo, a *finalidade* olhando do

centro da figura para as extremidades mostra como esses indivíduos utilizam as informações e se inserem junto as mídias, bem como em outros provedores de informação. (UNESCO, 2016).

A *compreensão* por sua vez menciona o aspecto relacionado ao conhecimento básico dessas pessoas, em tratativas sobre padrões éticos estabelecidos nas formas de mídias e outros provedores de informação e se *ajustada/amarrada* com a finalidade favorecerá a análise crítica, o uso ético da informação e da mídia. (UNESCO, 2016).

O *processo e a prática* demonstram claramente a sequência tomada pelas pessoas ao seguirem para a criação e utilização de informações e conteúdos midiáticos em benefícios e ética, com o intuito de integração em suas vidas social, política, cultural e pessoal desses jovens. (UNESCO, 2016).

Um público alfabetizado em mídias e na informação admitem uma posição crítica e verdadeira em relação a conceitos como de liberdade de opinião, expressão e comunicação, ainda de como sopesar o entendimento desses direitos na condução de suas próprias ações e condutas. (UNESCO, 2016).

2.2 *Cibercrimes*

A velocidade na qual as transformações virtuais acontecem hoje no mundo, incluindo as novas tecnologias disponibilizadas a qualquer ser humano, a capacidade de processamento de informações *on line*, com certeza altera o cenário das práticas criminosas ao redor do mundo.

Então, consequentemente se pode afirmar que tais condutas delituosas, desencadeadas em redes digitais, são decorrentes do mau uso da tecnologia e com isso ocasionam danos imensuráveis e de grave ordem, sejam de cunho social, moral, material, emocional e outros.

Em decorrência lógica os crimes virtuais estão sendo praticados num contexto diferente do que acontecem com os crimes tradicionais, o que pode conduzir a diferentes fatores para ambos envolvidos, ofensor e vítima (WEULEN *et al*, 2019).

Necessário se considerar neste estudo também as distinções entre as realidades fáticas dos países envolvidos em contextos criminais ao redor do mundo,

que foram estudados e nesse sentido, algumas nações como os EUA sofrem cerca de 60% dos volumes de *phishing* em todo o mundo, sendo as origens desses ataques de países como China, Rússia, Ucrânia e Brasil (KIGERL, 2016).

Ademais, o computador é o bem móvel mais utilizado e principal ferramenta de violação dos bens jurídicos tutelados pelo ordenamento jurídico brasileiro, sejam de cunho material ou mesmo imaterial, e ainda os delitos *ciber* são definidos como sendo próprios (puros) e impróprios (mistos), portanto, os crimes digitais próprios compreendem as condutas contra os sistemas informáticos, sendo os dados e impróprios são as condutas contra os tradicionais bens jurídicos com o uso de dispositivos informatizados pela *internet* ou mediante troca e armazenamento de arquivos eletrônicos (PIMENTEL, 2018).

O termo ideal para a ocorrência dos crimes eletrônicos pela sua equivalência com os *cibercrimes* se trata da expressão *crime cibernético*, objeto da versão em língua portuguesa oriundo da Convenção de Budapeste (2001), de boa literatura internacional e de área especializada do *Federal Bureau of Investigation* (FBI) (PIMENTEL, 2018).

O Brasil não é signatário da Convenção de Budapeste, porém esta ferramenta é atualmente a mais completa e usada nesse cenário virtual, um amplo instrumento jurídico utilizado frente às fraudes praticadas, por meio do uso de computadores (PIMENTEL, 2018).

No caso de punir um indivíduo criminoso que pratica um delito na *internet* contra um brasileiro, estando em sua casa na Alemanha? Da maneira atual em que os governos atuam é praticamente impossível punir um criminoso desse tipo, que é regido por outras legislações e é submetido a um Poder Soberano distinto, não respondendo perante às leis pátrias, sendo assim, permanecendo impune o crime diante da fragilidade dos ordenamentos jurídicos mundiais (RUTHERFORD, 2015).

Segundo dados do Norton Relatório de Crimes Cibernéticos (2018), esse tipo de crime é uma epidemia global silenciosa, cerca de 65% das pessoas já sofreram algum tipo de ataque cibernético, destacando a importância da Educação Digital nesse contexto. O impacto humano, quando os crimes ocorrem, 48% das pessoas se comunicam com o banco, 44% em contato com a polícia e apenas 34% entram em contato com o *website* ou o provedor de *e-mail* (NORTON, 2018).

Mais dados alarmam, o crime cibernético no Brasil é mais caro e é o terceiro mais lento de se resolver dentre todos os países pesquisados no estudo do Norton (RUTHERFORD, 2018).

Ainda o relatório Norton (2018) relata que no Brasil, China e na Nova Zelândia, a realidade é ainda mais ofensiva e ilícita, por possuir em média de 6 em cada 10 computadores infectados, os golpes triviais versam sobre *phishing*, fraude de cartão de crédito e furto de perfis em redes sociais, como outras modalidades de ilegalidades existentes, como os indivíduos que são predadores sexuais *on line*.

Devido a relevância do tema, a Comissão de Constituição e Justiça (CCJ) do Senado Federal aprovou no dia 12 de dezembro de 2018, o Projeto de lei Complementar (PLC) nº 110/2018 de autoria da Deputada Laura Carneiro/RJ, destinado a criação dos Juizados Especiais Criminais Digitais que serão responsáveis pela conciliação, instrução probatória de uma demanda de cunho cibernético, julgamento da lide e execução de sanções oriundas da sentença penal condenatória, portanto, versa sobre uma inovação legislativa, em virtude do aumento expressivo do número de casos oriundos de ações delitivas em ambiente cibernético (CONSULTOR JURÍDICO, 2018).

Por derradeiro, não restam dúvidas que a *internet* é um jardim propenso, vasto e muito florido, para as pessoas mal-intencionadas e direcionadas para o cometimento de infrações penais pelo mundo, sejam elas qual forem, em qual ambiente físico estiverem, contudo, surge a necessidade de uma regulamentação internacional eficiente, a fim de se alcançar o instituo da segurança jurídica, respeitando obviamente o Poder Soberano dos países do globo.

2.2.1 Crimes Próprios

É dever estatal da União *definir/tipificar* as condutas delitivas atuais diante do concreto avanço do parque tecnológico colocado à disposição das pessoas nos dias atuais, tendo em vista obviamente que contribui para uma notável evolução social, humana e negocial. Dessa forma há resultados práticos dessa utilização em massa das plataformas mediadas tecnologicamente, por isso é que o Direito tem o escopo de entender esse novo cenário, partindo do pressuposto de que o caráter jurídico está presente maciçamente na atividade cotidiana junto à rede pelos indivíduos (CARNEIRO, 2012).

Claro que existem falhas legislativas no arcabouço nacional de leis, bem como ausências de condutas criminosas que precisam ser devidamente tipificadas junto ao ordenamento jurídico brasileiro, fato esse que se alicerça devido ao elevado número de casos no Brasil, por isso da necessidade de providências legais urgentes a respeito dessa relevante temática.

Com relação aos crimes convencionais relacionados ao TIC e previstos na legislação pátria, infelizmente são insatisfatórios, no tocante a classificação dos delitos praticados contra o computador ou por meio dele frente às correntes modalidades criminosas que nasceram nesse contexto atual de mundo e que fazem realmente jus de serem definidos em leis especiais, com o intuito de garantia da ordem social, institucional e legal (CARNEIRO, 2012).

Portanto, o Direito e as Tecnologias da Informação e da Comunicação (TIC) devem estar em plena consonância funcional, a fim de disponibilizar segurança, praticidade e tranquilidade aos usuários da rede.

No Brasil esse assunto teve realmente sua relevância nas últimas décadas, inclusive com a Constituição Federal de 1988, que promulgou importantes leis que tratam sobre a competência estatal de assuntos e questões sobre TIC (CARNEIRO, 2012).

As práticas delituosas próprias são aquelas em que o autor da conduta criminosa se utiliza do computador como um sistema TIC e que é usado como objeto meio para consecução do crime cibernético. Nessa categoria de crimes está não só a invasão de dados não autorizados por terceiros (vítimas), mais toda a interferência em dados contidos junto as TIC (CARNEIRO, 2012).

Em palestra proferida o professor e doutrinador Damásio Evangelista de Jesus *apud* Aras (2001) entende a respeito do tema que os:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Portanto, nessa particularidade de crimes a invasão ilícita de dados, com a finalidade delituosa de corromper, adulterar e com isso realizar a inserção de dados inverídicos que atingem diretamente o software ou hardware da máquina. Assim os

crimes próprios que são também conhecidos como delitos puros se situam na posição de que apenas ocorrem em ambientes relacionados a TIC, ou seja, a execução e consumação da conduta criminosa acontecem nesse amplo meio digital disponibilizado a todos os indivíduos situados ao redor do mundo (ALMEIDA, 2015).

2.2.2 Crimes Impróprios

Diferentemente dos crimes puros os impróprios são aqueles em que a concretização da conduta ilícita ocorre não apenas se utilizando das TIC, como também de formas adversas e não necessariamente pelas vias virtuais colocadas à disposição dos homens, como exemplo emblemático de delito digital impuro, temos a pedofilia.

Oportuno e conveniente descrever acerca da palestra proferida pelo professor Damásio Evangelista de Jesus *apud* Aras (2001), a respeito do tema abordado:

> Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Tais classificações são de suma relevância, a fim de entender a evolução criminosa no mundo contemporâneo, seus aspectos doutrinários, sua dinâmica operacional, bem como se desenvolve junto ao uso da rede de *internet*.

Ainda que sejam cometidos crimes, por meio de uma máquina (computador), há de se identificar aqui que o bem jurídico tutelado e ofendido na empreitada delitiva poderá ser afetado de inúmeras maneiras e não apenas com o uso pontual do computador, pois o equipamento não é essencial para que a conduta criminosa alcance o mundo dos *fatos/físico*, portanto, em desacordo com as TIC (ORRIGO; FILGUEIRA, 2015).

Em decorrência lógica seguem alguns exemplos de delitos tipificados no ordenamento jurídico pátrio, como os crimes bem conhecidos pela grande maioria das pessoas e que se configuram contra a honra da vítima, conforme descreve os artigos 138 (calúnia), 139 (difamação), 140 (injúria), descritos junto ao Capítulo V – Dos Crimes contra a Honra e os delitos mencionados nos artigos (146)

constrangimento ilegal, 147 (ameaça) e 307 (falsa identidade), todos do Código Penal Brasileiro (JORGE, 2011).

Na situação de uma exposição não consensual de fotos, por exemplo, que caracterizam a intimidade de pessoas (pornografia) em redes sociais, que nada mais é do que a distribuição de vídeos que foram veiculados, contendo imagens e sons do indivíduo, obtidos de maneira clandestina ou mesmo até consensual no decorrer da atividade de cunho sexual, se tratando inclusive de local privativo, mas que foi lançado a público sem qualquer anuência de um dos envolvidos no ato.

No caso específico do *Ciberbullying* é o tipo penal que pode ser praticado de várias formas, por isso se mostra uma modalidade de crime em que vários profissionais, de áreas distintas inclusive, como educadores em geral, juízes, promotores de justiça, delegados de polícia, psicólogos, sociólogos e pesquisadores se preocupam em conhecer o comportamento e o fundamento dessa conduta devassadora denominada de *bullying.* Essa prática se enquadra na modalidade de delito impróprio e Tribunais de alguns estados brasileiros proferiram julgamentos entendendo pela procedência do dano moral requerido, em virtude de casos relacionados a essa prática, provenientes de sites de relacionamentos ou TIC e que ocasionou profunda lesão a honra das vítimas.

2.2.3 *Ciberbullying*

As Tecnologias da Informação e da Comunicação, conhecidas pela sigla (TIC) se mostram cada vez mais presentes no dia a dia das empresas e dos cidadãos em geral, inclusive agregando valor em negócios, operações bancárias, incluindo alterações em rotinas empresariais e em outros aspectos de relevância na vida cotidiana das pessoas (MPF, 2018).

Porém, há de se entender que esses recursos eletrônicos não estão presentes apenas na seara empresarial e dos cidadãos, mas sim de indivíduos *mal-intencionados/maliciosos*, que utilizam a TIC, para uma finalidade criminosa como os conhecidos delitos de estelionato, furto mediante fraude, pornografia de menores de idade, *Ciberbullying* dentre outros.

O *bullying*, por exemplo, que na verdade se trata de uma ação de cunho ofensivo, injusto, irregular, cruel e criminosa, que abarcam humilhações, *violência on line*, intimidações, chantagem e em outras oportunidades até o compartilhamento de

imagens e fotos íntimas de menores de idade via rede de *internet*. Ademais, englobam também os âmbitos escolares, profissionais (trabalho), vizinhança local (residência) e até no seio familiar do menor impúbere.

O escopo principal do *bullying*, se trata em proporcionar o efetivo desconforto (violência) de caráter físico, psíquico contra a criança e adolescente. No caso do *Ciberbullying* (nomenclatura moderna) as crianças não são as únicas vítimas, esse mal persegue inclusive indivíduos adultos, no entanto, esta proposta mira a abrangência de *crianças/adolescentes* no intervalo de 12 a 18 anos de idade.

O fato é que esses garotos representarão em um futuro muito próximo e oportuno junto à sociedade, pessoas com uma notável baixa autoestima, incluindo outros sintomas oriundos da prática ofensiva do *Ciberbullying,* que acompanhados possam eclodir possíveis cenários envolvendo tratativas de vingança a todo custo, como os menores que adentraram as escolas nos EUA armados vitimando alunos, docentes e funcionários desses estabelecimentos escolares.

A vítima do *Ciberbullying*, problemática moderna da sociedade, tem sua honra, dignidade humana, liberdade de expressão, intimidade, imagem e privacidade, ou seja, bens jurídicos que são devidamente protegidos por disposições legais vigentes no Brasil, sendo que essas intolerâncias desses indivíduos agressores tornam para a potencial vítima do *bullie,* simplesmente impossível de conviver de maneira favorável e harmoniosa, trazendo ainda consequências como a plena ausência de paz de espírito, a tranquilidade espiritual e outros.

A *internet* se mostra uma poderosa arma para assediar, ameaçar e causar intimidação em pessoas, por isso vigora a Lei nº 13.185/2015, que instituiu o Programa de Combate à Intimidação Sistemática (*Bullying*) e seus objetivos legais, conforme descrito no artigo 2.º

> Artigo 1º Fica instituído o Programa de Combate à Intimidação Sistemática (***Bullying***) em todo o território nacional.
> § 1º No contexto e para os fins desta Lei, considera-se intimidação sistemática (***bullying***) todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas.
> § 2º O Programa instituído no ***caput*** poderá fundamentar as ações do Ministério da Educação e das Secretarias Estaduais e Municipais de Educação, bem como de outros órgãos, aos quais a matéria diz respeito.

Artigo 2º Caracteriza-se a intimidação sistemática (***bullying***) quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação e, ainda:
I - ataques físicos;
II - insultos pessoais;
III - comentários sistemáticos e apelidos pejorativos;
IV - ameaças por quaisquer meios;
V - grafites depreciativos;
VI - expressões preconceituosas;
VII - isolamento social consciente e premeditado;
VIII - pilhérias.
Parágrafo único. 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.
Artigo 3º A intimidação sistemática (***bullying***) pode ser classificada, conforme as ações praticadas, como:
I - verbal: insultar, xingar e apelidar pejorativamente;
II - moral: difamar, caluniar, disseminar rumores;
III - sexual: assediar, induzir e/ou abusar;
IV - social: ignorar, isolar e excluir;
V - psicológica: perseguir, amedrontar, aterrorizar, intimidar, dominar, manipular, chantagear e infernizar;
VI - físico: socar, chutar, bater;
VII - material: furtar, roubar, destruir pertences de outrem;
VIII - virtual: depreciar, enviar mensagens intrusivas da intimidade, enviar ou adulterar fotos e dados pessoais que resultem em sofrimento ou com o intuito de criar meios de constrangimento psicológico e social.
Artigo 4º Constituem objetivos do Programa referido no ***caput*** do art. 1º:
I - prevenir e combater a prática da intimidação sistemática (***bullying***) em toda a sociedade;
II - capacitar docentes e equipes pedagógicas para a implementação das ações de discussão, prevenção, orientação e solução do problema;
III - implementar e disseminar campanhas de educação, conscientização e informação;
IV - instituir práticas de conduta e orientação de pais, familiares e responsáveis diante da identificação de vítimas e agressores;
V - dar assistência psicológica, social e jurídica às vítimas e aos agressores;
VI - integrar os meios de comunicação de massa com as escolas e a sociedade, como forma de identificação e conscientização do problema e forma de preveni-lo e combatê-lo;
VII - promover a cidadania, a capacidade empática e o respeito a terceiros, nos marcos de uma cultura de paz e tolerância mútua;
VIII - evitar, tanto quanto possível, a punição dos agressores, privilegiando mecanismos e instrumentos alternativos que promovam a efetiva responsabilização e a mudança de comportamento hostil;
IX - promover medidas de conscientização, prevenção e combate a todos os tipos de violência, com ênfase nas práticas recorrentes de intimidação sistemática (***bullying***), ou constrangimento físico e

> psicológico, cometidas por alunos, professores e outros profissionais integrantes de escola e de comunidade escolar.
> Artigo 5º É dever do estabelecimento de ensino, dos clubes e das agremiações recreativas assegurar medidas de conscientização, prevenção, diagnose e combate à violência e à intimidação sistemática (***bullying***).
> Artigo 6º Serão produzidos e publicados relatórios bimestrais das ocorrências de intimidação sistemática (***bullying***) nos Estados e Municípios para planejamento das ações.
> Artigo 7º Os entes federados poderão firmar convênios e estabelecer parcerias para a implementação e a correta execução dos objetivos e diretrizes do Programa instituído por esta Lei.
> Artigo 8º Esta Lei entra em vigor após decorridos 90 (noventa) dias da data de sua publicação oficial (BRASIL, 2015).

Na data de 07 de abril é considerado do Dia Nacional de Combate a este tipo de violência na escola (*bullying)*. A *Safernet* e o UNICEF lançaram uma campanha de conscientização pelo combate a esta espécie de violência conhecida popularmente como *bullying* (SAFERNET, 2020).

Ainda existe a Lei nº 13.663/18, que institui a inclusão de medidas de conscientização, de prevenção e de combate a todos os tipos de violência, bem como em especial a intimidação sistemática (***bullying***), no âmbito das escolas, a promoção da cultura da paz nas dependências físicas dos estabelecimentos de ensino do Brasil.

> Artigo 1º O **caput** do art. 12 da Lei nº 9.394, de 20 de dezembro de 1996 , passa a vigorar acrescido dos seguintes incisos IX e X:
> "Art.12.....
> IX - promover medidas de conscientização, de prevenção e de combate a todos os tipos de violência, especialmente a intimidação sistemática (**bullying**), no âmbito das escolas;
> X - estabelecer ações destinadas a promover a cultura de paz nas escolas." (NR)
> Artigo 2º Esta Lei entra em vigor na data de sua publicação. (BRASIL, 2018).

A *Safernet* é uma ONG (Organização Não Governamental) no Brasil, que promove a defesa dos direitos humanos junto à *internet*, atuando na orientação e educação das crianças, adolescentes e jovens, pais e educadores sobre o uso responsável e seguro da rede de *internet* (SAFERNET, 2020).

Enquanto a UNICEF é regida pelos direitos da criança e trabalha para que essas conquistas (direitos) se convirjam diretamente em princípios éticos, morais permanentes e em códigos de conduta internacionais com o forte escopo nas

crianças. A sigla significa Fundo das Nações Unidas para a Infância, em inglês *"United Nations Children's Fund",* é uma agência oriunda das Nações Unidas. A UNICEF é a única organização mundial que se dedica especificamente às crianças (UNICEF, 2018).

Óbvio que a atual tecnologia evoluiu a vida e o conforto das pessoas, proporcionando padrões elevados de vida, isso é claro a um nível mundial, mas também está com certeza destoando outras escaladas criminosas que antes não se falava a respeito, sendo que se quer havia notícias, que dentre elas está um dos delitos mais odiosos da sociedade contemporânea, a *pornografia infanto-juvenil,* como outra forma de violência infanto juvenil e que se insere no contexto do *Ciberbullying, pois também* versa sobre uma agressividade intencional que causa dor, angústia se inserindo em uma relação desigual de poder.

Tal modalidade delitiva consiste na exposição corporal de forma não consensual das vítimas, captadas por meio de imagens a exposição pornográfica consiste na distribuição de imagens, sons oriundos de atos sexuais, vídeos publicados sem obviamente a autorização do menor impúbere (BARRETO; ARAÚJO, 2017).

Muitas vezes a obtenção de imagens de um cenário privado é realizada por via de recursos clandestinos no transcorrer de ato sexual ou mesmo de maneiras autorizadas pela vítima, mas o compartilhamento desse material ocorreu infelizmente sem o consentimento de um dos envolvidos (BARRETO; ARAÚJO, 2017).

Nesse contexto entra o termo conhecido como *pornografia de vingança,* que consiste na divulgação em rede de *internet* de materiais que abrangem fotos, imagens, vídeos, que possuem caráter privado de certa pessoa (relacionamentos amorosos privados e até sigilosos), sem é claro de sua anuência e que contenha cenas de nudez, sexo, exposições pessoais diversas, cujo ideal do autor será sempre a difamação perante o alto poder de atingimento da *internet* (BARRETO; ARAÚJO, 2017).

A viralização que a rede de *internet* causa é inimaginável ao homem médio, portanto, a conduta do autor destrói a *boa reputação/fama* da pessoa atingida (vítima), como também causa enormes *estragos/feridas* emocionais, sociais e principalmente em ambiente escolar, sendo por repetidas vezes lembrada a distribuição de materiais via rede de *internet* (BARRETO; ARAÚJO, 2017).

As vítimas geralmente são individualizadas, por isso, são devidamente reconhecidas pelo público internauta, pois os dados e informações veiculados inclusive nas redes sociais são suficientes e amarram a determinado indivíduo sem sombras de dúvidas, denegrindo sua imagem pessoal perante a sociedade em geral, ao ambiente de trabalho e escolar (BARRETO; ARAÚJO, 2017).

Tal apresentação desse tipo de conteúdo junto à *internet* na maioria das vezes tem origem em autores inescrupulosos como parceiros íntimos, familiares, amigos de escola, outros e também desconhecidos (BARRETO; ARAÚJO, 2017).

A *divulgação/exposição* de materiais íntimos não autorizados em que participam crianças e adolescentes é considerado ato criminoso, segundo o Estatuto da Criança e Adolescente (ECA) (BARRETO; ARAÚJO, 2017).

A possibilidade de rastreamento de ações de divulgação e exposição de materiais não autorizados junto a rede de *internet* é hoje uma realidade, pois toda a navegação, consulta, produção de conteúdo, cliques em sites e links diversos na rede, fornecem em potencial um rastro, registro, que permanece sensível de ser obtido devido a existência de intrigados bancos de dados (BRUNO, 2016).

O anonimato nas relações de comunicação e informação desenvolvido no ambiente *ciber,* é uma forma em que os autores da prática de *Ciberbullying* acreditam na conhecida impunidade, mas as mesmas TIC que propiciam esse ocultismo, possibilitam também formas de identificação de indivíduos envolvidos nessa conduta, pois as plataformas digitais capturam dados dos indivíduos como os rastros deixados pelo acesso (BRUNO, 2013).

Em específico o comportamento do autor dessa prática ofensiva demonstra um comportamento agressivo e intencionalmente perverso via *internet*, muitas vezes de maneira reiterada (perseguição *contínua/insistente*) e por meio de uma relação interpessoal assimétrica, evidenciada por explícita dominação (BASTOS *et al.,* 2016).

Os resultados dessas condutas lamentáveis realizadas em ambiente digital, refletem no campo da pessoalidade humana do adolescente, inclusive podendo ser tão mais agressiva do que no campo da realidade fática, pois em ambientes reais, a prática seria nitidamente presenciada por aqueles indivíduos que estariam próximos ao autor e a vítima, enquanto que na rede de *internet* o *Ciberbullying* que é explicitado por agressões, humilhações e outras condutas, proporcionaria

resultados que não teriam limites geográficos imagináveis, ou seja, vulnerabilizaria completamente o sujeito (MISTURA, 2018).

Os danos se estendem desde o aspecto psicológico do indivíduo até sinais de baixa autoestima, com desenvolvimento inclusive de problemas patológicos, esse público, vítima do *Ciberbullying* manifesta temor de se expressar publicamente, possuem fobia social, quadros depressivos, evitam o contato com pessoas e principalmente necessitam da atenção de profissionais experientes e especialistas de algumas áreas, a psicologia é uma delas (MISTURA, 2018).

2.2.3.1 O *Ciberbullying* em Época de Pandemia da Covid-19

A doença conhecida por Covid-19 trata-se de uma enfermidade viral declarada pela Organização Mundial da Saúde (OMS), na data de 11 de março de 2019. O causador dessa moléstia foi identificado como *coronavírus* (sars-cov-2) e se transformou em uma pandemia partindo inicialmente de uma epidemia local no continente asiático (DESLANDES; COUTINHO, 2020).

A proliferação de casos da doença no mundo ocorreu de maneira exponencial, com isso a OMS entendeu e aconselhou aos países que praticassem a metodologia do isolamento social, como medida de eficiência no combate a expansão do vírus no planeta (DESLANDES; COUTINHO, 2020).

Com isso a rede de *internet* se tornou o único meio adequado à época e claro, porque está colocado à disposição de muitos indivíduos, para a realização de trabalhos, tarefas e também em contatos sociais entre amigos, familiares e para outros fins (DESLANDES; COUTINHO, 2020).

Contudo, houve um aumento significativo das interações entre pessoas no contexto do ambiente digital, fazendo a sociabilidade digital avançar demasiadamente. Com isso outro efeito concreto foi a hiperexposição que na verdade abrange uma diminuição ainda maior das fronteiras entre o aspecto público e privado de indivíduos (DESLANDES; COUTINHO, 2020).

Assim as crianças e os adolescentes praticando ativamente o isolamento social, se renderam mais ainda a utilização das plataformas digitais disponíveis e consequentemente há a possibilidade real de aumento nas condutas delitivas de *Ciberbullying* (ABRACE, 2020).

Tais informações fazem todo o sentido se levar em conta o aumento de usuários da rede, claro de agressores e de vítimas. Com esse público na situação de isolamento social, ou seja, em casa o acesso aos aplicativos são feitos continuamente se comparados se estivessem, por exemplo, em ambiente escolar. (ABRACE, 2020).

Educadores também muitas vezes trabalhando de suas casas, por isso não dispõem de um contato pessoal real com esses estudantes, alvos de *Ciberbullying*, por essa razão as vítimas suportam e sofrem silenciosamente a agressão que em muitas situações poderiam ser divididas com professores, orientadores ou educadores em geral presentes no dia a dia escolar (ABRACE, 2020).

Mesmo em ambiente *on line* é de bom grado que os professores idealizem ideias que tragam interações positivas para esses jovens, incentivando a se exporem, por meio de atividades que tragam a manifestação das emoções humanas, o encontro com amigos pelas ferramentas digitais disponíveis como *Skype, FaceTime*, jogos e a demonstração através da conciliação harmônica desse atual cenário de caos e incertezas sanitárias (ABRACE, 2020).

Óbvio que a propagação do *coronavírus* alterou a rotina dos jovens trazendo um confinamento domiciliar indispensável, fundamental ao controle sanitário do vírus no mundo, essa nova dinâmica colocada no seio das famílias, por óbvio desencadeou o cometimento de crimes pelos indivíduos mal-intencionados e dentre eles o *Ciberbullying* (USO..., 2020).

A *Europol* (Agência de Inteligência da Europa), por exemplo, dispôs que houve um aumento considerável no exercício de atividades *on line* de pessoas que buscam conteúdos de materiais relativos a abuso sexual infantil, o relatório mencionou que entre os dias 17 e 24 de março de 2020, portanto, em época de pandemia da Covid-19, foi registrada uma alta de 25% no número de conexões de download de material impróprio na Espanha e em outros países do continente europeu (USO..., 2020).

Nesse momento os pais desempenham um papel urgente e de extrema valia, pois podem exercer sistematicamente uma supervisão de acessos as plataformas digitais de seus filhos, inclusive utilizando o diálogo como ferramenta principal, salientar da importância de estar seguro no ambiente digital, das exposições desnecessárias, em quem confiar e caso esteja acontecendo algo errado

trazer ao conhecimento desses responsáveis legais (USO..., 2020), por isso da importância do folheto digital, produto desenvolvido neste trabalho de mestrado.

O cenário é idêntico ao do pai que acompanha ativamente seu filho ao atravessar a rua movimentada por carros e pessoas em uma grande capital. Por isso que o trato com os filhos a respeito de segurança na *internet* é importante, para evitar que se tornem vítimas fáceis da violência *on line* (USO..., 2020).

Por fim, conversar com crianças e adolescentes sobre segurança *ciber* é obrigatório, avaliar jogos e aplicativos antes de baixarem, configurações de privacidade no nível máximo no uso em geral da rede são ferramentas valiosas, como também o monitoramento através do uso da *internet* em uma sala aberta para todos da casa e sempre explicar que o material que foi postado em forma de vídeo, imagem ficará em definitivo hospedado na *internet* (USO..., 2020), são atos de relevância e pertinência na prevenção do *Ciberbullying*.

2.2.4 Lei nº 13.718/18 que trata de Crimes de Importunação Sexual e Divulgação de Cenas de Estupro

A Lei nº 13.718/18, de 24 de setembro de 2018, foi sancionada em um contexto na qual o exercício temporário do cargo de Presidente da República foi exercido pelo Sr. Presidente do Supremo Tribunal Federal Ministro José Antônio Dias Toffoli.

Os delitos descritos na referida lei tratam de atos libidinosos na presença de outrem e de maneira não consentida, com o escopo de satisfazer a própria lascívia ou ainda de terceiro interessado.

Ainda a lei acrescentou novas figuras criminais no Código Penal Brasileiro e transformou em crime a divulgação, por meio das plataformas digitais TIC, cenas de sexo, pornografia ou mesmo de nudez.

> Artigo 1º Esta Lei tipifica os crimes de importunação sexual e de divulgação de cena de estupro, torna pública incondicionada a natureza da ação penal dos crimes contra a liberdade sexual e dos crimes sexuais contra ***vulnerável***, estabelece causas de aumento de pena para esses crimes e define como causas de aumento de pena o estupro coletivo e o estupro corretivo.
> Artigo 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
> “ **Importunação sexual**

Artigo 215-A Praticar contra alguém e sem a sua anuência ato libidinoso com o objetivo de satisfazer a própria lascívia ou a de terceiro:
Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o ato não constitui crime mais grave."
"Artigo 217-A. .....
§ 5º As penas previstas no **caput** e nos §§ 1º, 3º e 4º deste artigo aplicam-se independentemente do consentimento da vítima ou do fato de ela ter mantido relações sexuais anteriormente ao crime." (NR)
" **Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia**
Artigo 218-C Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, ***publicar ou divulgar, por qualquer meio*** - inclusive por meio de comunicação de massa ou ***sistema de informática ou telemática*** -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:
Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
Aumento de pena
§ 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.
Exclusão de ilicitude
§ 2º Não há crime quando o agente pratica as condutas descritas no **caput** deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos."
"Artigo 225 Nos crimes definidos nos Capítulos I e II deste Título, procede-se mediante ação penal pública incondicionada.
Parágrafo único. (Revogado)." (NR)
"Artigo 226. .....
II - de metade, se o agente é ascendente, padrasto ou madrasta, tio, irmão, cônjuge, companheiro, tutor, curador, preceptor ou empregador da vítima ou por qualquer outro título tiver autoridade sobre ela;
IV - de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado:
Estupro coletivo
a) mediante concurso de 2 (dois) ou mais agentes;
Estupro corretivo
b) para controlar o comportamento social ou sexual da vítima." (NR)
"Artigo 234-A. .....
III - de metade a 2/3 (dois terços), se do crime resulta gravidez;
IV - de 1/3 (um terço) a 2/3 (dois terços), se o agente transmite à vítima doença sexualmente transmissível de que sabe ou deveria saber ser portador, ou se a vítima é idosa ou pessoa com deficiência" (NR)
Artigo 3º Revogam-se:
I - o parágrafo único do art. 225 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

> II - o artigo 61 do Decreto-Lei nº 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais).
> Artigo 4º Esta Lei entra em vigor na data de sua publicação. (BRASIL, 2018).

A pornografia de vingança é uma modalidade que envolve um conteúdo de cunho sexual, portanto, íntimo e foi compartilhado nas plataformas digitais de informação e comunicação sem o necessário consentimento da vítima, por pessoa que é de sua confiança ou mesmo de sua intimidade. O intuito do autor dessa conduta é com certeza proporcionar constrangimentos, embaraços, até ameaças e um profundo incômodo.

Claro que tais divulgações são impróprias, inoportunas, injustas, cruéis e ofensivas, mas na verdade, são literalmente considerados vazamentos de imagens íntimas, que causam danos inimagináveis, irremediáveis a pessoa humana desse público alvo, inclusive porque destrói a honra da vítima, abrangendo inclusive as suas saúdes física, mental e repercutindo em alguns efeitos psicossomáticos.

O *Cibebullying* de cunho sexual é uma prática que acontece muito no mundo moderno, inclusive o artigo 218-C, do Código Penal, menciona uma conduta após a obtenção de uma foto e que a disseminação dessa imagem em um grupo de rede social, por exemplo, tenha ocorrido sem o consentimento da outra parte, então quando a troca de fotos eróticas e sensuais acontece entre as partes, não há aqui a incidência desse artigo de lei.

Assim o *Ciberbullying* infelizmente se torna uma conduta relevante no cenário moderno, a tendência é que praticamente todos tenham acesso a rede de *internet*, ainda considerando o avanço e crescimento tecnológico das plataformas de informação e comunicação, qualquer material digital enviado seja mensagem, vídeo ou foto, que podem terminar sendo publicados e expostos ao mundo, trazendo infinitas perturbações a vítima.

2.3 Privacidade de Dados Pessoais

A privacidade de informações e dados pessoais, nada mais é do que a exigência de indivíduos pertencentes a uma sociedade, de órgãos, instituições e empresas particulares ou públicas, de terem seus dados e informações transmitidos a terceiros de maneira restritiva, ou seja, somente nas hipóteses especificadas em

legislação específica, ainda essa modalidade de privacidade é tida como uma das mais relevantes nos cenários éticos, sociais, legais, morais e políticas do ciclo da informação (DA SILVA JUNIOR *et al.,* 2020).

Ainda, se analisada a questão de uma forma progressiva, com certeza se identificará como um mecanismo de controle seletivo de dados sociais, interpessoais e outros, concernentes ao acesso as pessoas de um determinado grupo e/ou a si próprio. Um jovem no uso diário de seu *smartphone*, por exemplo, autoriza o download de aplicativos (*apps*) como *Google Play* e outros sem se preocupar com tratativas de segurança durante a instalação desses programas (DA SILVA JUNIOR *et al.,* 2020).

O simples ato de instalação de *apps* no aparelho telefônico, sem as cautelas necessárias e atinentes as questões de segurança, como a habilitação de controles de segurança do smartphone, o torna um possível alvo de ataques em desfavor da segurança e da privacidade do usuário (DA SILVA JUNIOR *et al.,* 2020).

A Lei Geral de Proteção de Dados (LGPD) nº 13.709/18 sancionada pelo Excelentíssimo Senhor Presidente da República Federativa do Brasil Sr. Michel Temer, na data de 14 de agosto de 2018, estabeleceu que o fim da *vacatio legis*, ou seja, o prazo final de adequação dos envolvidos no cenário digital (governo, empresas e a sociedade civil) que está previsto para o dia 16 de fevereiro de 2020, quando passará então a ter plena eficácia no cenário jurídico nacional.

Contudo, no mês de dezembro de 2018 foi editada a Medida Provisória (MP) nº 869/18, que estendeu por mais 6 meses, passando a ser de 24 meses o prazo de *vacatio legis* da LGPD, em virtude da vigência anterior que era de 18 meses, portanto, agora a lei entrará em vigor segundo a MP, no dia 14 do mês de agosto de 2020.

No entanto, a Medida Provisória nº 959, de 29 de abril de 2020, publicada no Diário Oficial da União de 30 de abril de 2020, estabelece a prorrogação da *vacatio legis* para o dia 03 de maio de 2021, portanto, a Lei nº 13.709, de 14 de agosto de 2018, não entrará em vigor de imediato.

Com relação as sanções estas serão aplicadas a partir de 1º de agosto de 2021 e esta data foi definida, por meio da Lei nº 14.010, de 10 de junho de 2020. No dia 26 de agosto de 2020 o Senado Federal entendeu prejudicado o artigo 4º, da MP nº 959, na prática entendesse que o adiamento da LGPD proposto pela MP nº 959 não acontecerá mais.

O Excelentíssimo Sr. Presidente da República possui o prazo de 15 dias após o recebimento para sanção ou veto da MP nº 959, que se converteu no Projeto de Lei Complementar nº 034/2020.

A LGPD se espelhou no Regulamento Geral de Proteção de Dados europeu (EPM, 2020). Possui seus alicerces calcados nos direitos fundamentais da privacidade, liberdade, livre iniciativa, desenvolvimento tecnológico e econômico do Brasil o que traz proteção, transparência e regulamentação acerca dos dados pessoais dos cidadãos no país, abrangendo os âmbitos particulares e públicos (SOMADOSSI, 2018).

Os dados pessoais apenas deverão ser coletados e utilizados minimamente segundo as finalidades específicas que determinaram seu tratamento, ainda ser objeto de ciência formal dos cidadãos titulares desses dados. A regulamentação define como dado pessoal qualquer informação que identifique diretamente ou torne identificável uma pessoa natural e tratamento, como toda operação realizada com dados pessoais, tais como a coleta, utilização, acesso, transmissão, processamento, arquivamento, armazenamento, transferência, ou seja, a lei consigna 20 verbos e ações que explicitam formas de tratamentos diversas de dados, nos termos do artigo 5º, X, da Lei nº 13.709/18. (SOMADOSSI, 2018).

Outra vertente interessante versa sobre toda e qualquer operação de tratamento de dados pessoais, realizada em território nacional, seja por pessoa física ou jurídica de direito público ou privado, cujos titulares estejam localizados no Brasil ou tenham por finalidade a oferta de produtos ou serviços no mercado nacional estarão sujeitos a abrangência da LGPD, incluindo a exigência do consentimento expresso (manifestação livre, informada e inequívoca de concordância com o tratamento de dados pessoais) do usuário titular dos dados (SOMADOSSI, 2018).

A privacidade de dados possui algumas vertentes presentes junto a literatura, como a privacidade como um direito humano, da informação, mercadoria e a privacidade tida como um estado de acesso limitado e aquela reconhecida como a capacidade de controlar os dados sobre si mesmo (DA SILVA JUNIOR *et al.,* 2020).

A lei trouxe a criação da Autoridade Nacional de Proteção de Dados (ANPD), um órgão ligado diretamente à Presidência da República, cujo intuito é fiscalizar o cumprimento do diploma legal estabelecido, aplicar sanções (multas pelo descumprimento legal que podem, inclusive, chegar ao patamar de 50 milhões de

reais), editar normas e procedimentos e comunicar as autoridades competentes (Ministério Público), acerca do cometimento de infrações penais.

São fundamentos da LGPD, segundo preleciona o artigo 2°, *os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania* pelas pessoas naturais, dessa forma ensejam medidas educativas digitais efetivas, no tocante, a ensinos e aprendizados virtuais dispostos, por meio de políticas públicas contundentes, a fim de minimizar práticas criminosas gerando com isso segurança da informação ao país (BRASIL, 2018).

Ainda, a LGPD (BRASIL, 2018) apresenta ao Brasil um bom arcabouço de medidas legais, que regulamentam, disciplinam, sancionam e exigem a adequação das empresas, governo e sociedade civil a um sítio sacramentado de boas práticas, governança corporativa, *compliance*, trazendo o aspecto do princípio da segurança jurídica, bem como investimentos em segurança digital externos, pois o ambiente de negócios brasileiro está respaldado com um lastro confiável de segurança cibernética e com isso atrairá certamente mais investidores.

Em consonância com o aspecto da segurança da informação o Senado Federal aprovou no dia 02 de julho de 2019, a PEC (Proposta de Emenda Constitucional) nº 17/19 de autoria do Senador Eduardo Gomes/TO e relatado pela Senadora Simone Tebet/MS, portanto, uma novidade no arcabouço jurídico legislativo brasileiro, mais o fato é que essa PEC trata da proteção de dados pessoais disponíveis junto aos meios virtuais, no entanto, a proposta tem o escopo de *alcançar o âmbito constitucional*, ou seja, as tratativas a fim de legislar sobre a temática será da União e não dos outros entes federativos como estados e municípios. Hoje existem leis, normas e jurisprudências que reconhecem o direito à privacidade do indivíduo, que na verdade são apenas normas de níveis infraconstitucionais, por isso da necessidade dessa PEC.

Concernente as garantias individuais trazidas pela Constituição Federal de 1988, a proteção de dados pessoais deverá ser considerada uma extensão da proteção a intimidade dos cidadãos, com o intuito de resguardar a inviolabilidade dos dados junto à rede mundial de *internet*.

A LGPD, portanto, passou a vigorar no dia 18 de setembro de 2020, com a sanção da Lei nº 14.058/2020, que teve seu respaldo legal na Medida Provisória nº 959/20. Essa MP foi editada no mês de abril de 2020, sendo que o governo Jair Bolsonaro incluiu o artigo 4º que trouxe o adiamento do início da vigência para maio

de 2021, porém em análise conjunta pelo Congresso Nacional tal dispositivo não foi considerado.

Por fim, o desafio de manter a privacidade de dados e informações está lançado, pelo aumento exponencial de informações de ordem pessoal no mundo contemporâneo, principalmente nos meios digitais combinados com as ascensões tecnológicas que presenciamos no dia a dia (DA SILVA JUNIOR *et al.,* 2020).

2.3.1 O tratamento de Dados de Crianças e Adolescentes no âmbito da Lei Geral de Proteção de Dados Brasileira (LGPD)

O fato da globalização de acesso à rede de *internet* revolucionou a comunicação com as pessoas de real *significado/importância*, sejam esses familiares e/ou amigos, enfim trouxe um amplo acesso das TIC, sem, contudo, levar em conta as distâncias territoriais na qual cada desses indivíduos está devidamente localizado.

Ainda deverá ser observado, que de acordo com o entendimento da revista *The Economist,* salientou que *"o recurso mais valioso do mundo contemporâneo não se trata mais do petróleo, mas sim de dados".*

Oportuno e conveniente mencionar que segundo a Constituição Federal de 1988, a Convenção das Organizações das Nações Unidas (ONU) sobre os Direitos das Crianças e do Estatuto da Criança e Adolescente (ECA), que tratam da proteção do menor impúbere, é dever de todos, especialmente do Estado Brasileiro, família e da sociedade civil (EPM, 2020).

Assim todas as pessoas envolvidas nessa cadeia de tutela devem atender o melhor interesse das crianças e adolescentes, portanto, pais, empresas que administram dados pessoais, professores, estabelecimentos escolares e o Estado, enfim a sociedade civil envolvida como um todo, devem estar conscientes de suas responsabilidades nessa toada fundamental de proteção (EPM, 2020).

Segundo o relatório da UNICEF (Fundo das Nações Unidas para a Infância) de 2018 trouxe a preciosa informação de que a cada segundo duas crianças acessam a rede de *internet* pela primeira vez e esse montante corresponde ao valor de 175 mil novos usuários/dia (UNICEF, 1990).

Tanto as crianças como os adolescentes participam ativamente de locais como escolas, academias, jogos *on line*, aplicativos, clubes, hotéis e sites diversos

que coletam dados digitais de ordem pessoal e que deixam a segurança dos jovens em risco constante, portanto, vulneráveis, pois na visita a um site de jogos *on line*, o usuário com certeza terá monitorado suas pegadas digitais (UNICEF, 1990).

Dessa forma há a necessidade de reconsiderar os aspectos de proteção, informação, segurança e transparência, abordados pela LGPD, a fim de que os atingidos (crianças e adolescentes) reclamem sua real condição de hipossuficiência garantida constitucionalmente, bem como pelo ECA (Estatuto da Criança e do Adolescente) e outras legislações pertinentes.

2.3.2 A Singular Tutela de Crianças e Adolescentes

Claro que ao se tratar de aspectos que envolvem a proteção de menores impúberes (crianças e adolescentes), temos algumas legislações específicas a respeito da temática, como por exemplo, a Constituição Federal de 1988, o ECA, a Convenção sobre os Direitos da Criança com status de Tratado Internacional de Proteção de Direitos Humanos (EPM, 2020).

Quadro 1 – Legislações Específicas que Abrangem e Alcançam o Público Alvo

CF - Constituição Federal de 1988
ECA – Estatuto da Criança e do Adolescente
Convenção das Organizações das Nações Unidas (ONU) sobre os Direitos das Crianças
Lei nº 13.185/2015, que institui o Programa de Combate à Intimidação Sistemática (***Bullying***)
Convenção sobre os Direitos da Criança com status de Tratado Internacional de Proteção de Direitos Humanos

Fonte: Autor (2020)

A Constituição Federal menciona sua abordagem específica sobre o assunto, disposta junto ao artigo 227, salientando que:

> Artigo 227 - É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. (Redação dada Pela Emenda Constitucional nº 65, de 2010) (BRASIL, 2018).

Assim é evidente que a C.F de 1988 observa que os jovens são pessoas humanas de direito, pois possuem uma condição peculiar, no tocante, ao seu desenvolvimento, bem como pela atenção necessária com a prioridade constitucional elencada. Inclusive, é concedida a este público a integralidade de garantias, associadas aos direitos fundamentais, trazendo para esse rol o direito o nome, a informação, o lazer, intimidade e a vida privada (EPM, 2020).

O Brasil promulgou a Convenção sobre os Direitos da Criança (UNICEF), sem nenhuma ressalva, isso por meio do Decreto nº 99.710/1990, portanto esta legislação possui a condição de norma supralegal no âmbito do ordenamento jurídico nacional e diante desse contexto as legislações não deverão contradizer os ditames, princípios e os rumos explanados junto a Convenção (EPM, 2020).

Segundo a Convenção sobre os Direitos da Criança, o documento menciona que criança está conceituada como “todo ser humano com menos de 18 anos de idade, a não ser que, pela legislação aplicável, a maioridade seja atingida mais cedo” (EPM, 2020).

Já o ECA trata do tema referente a criança o definindo como sendo a pessoa humana de até 12 anos de idade incompletos e o adolescente como o indivíduo entre 12 e 18 anos de idade.

Mas como acontece então a tutela da LGPD em referência ao caso desses indivíduos vulneráveis ora mencionados. É claro que nessa seara ocorre a fiel proteção, aliás em sua integralidade, sendo que as pessoas (criança e adolescente) serão objeto da narrativa da legislação em vigor e que abarca a especial proteção da real dimensão dos interessados (EPM, 2020).

A ideia aqui não é impossibilitar por completo o tratamento de dados pessoais de crianças e adolescentes, muito menos a negativa, pois dessa forma estaria se tolhendo os direitos desses indivíduos de participarem ativamente da sociedade da informação e da comunicação, no entanto, seus dados deverão ser manipulados com cautela, apenas em cenários e situações de finalidade exclusiva, aliás a LGPD

menciona em seu artigo 14, parágrafo 4º, que os menores impúberes não terão o encargo de fornecer seus dados pessoais como condição para participarem de jogos virtuais, aplicações variadas de *internet* ou outras atividades digitais, com exceção daquelas estritamente necessárias ao desenvolvimento da atividade (EPM, 2020).

Portanto, a LGPD é uma legislação que respeita à vontade individual do jovem, seu direito e sua inclusão no meio digital moderno, aliado à sua condição peculiar de vulnerabilidade que está protegida constitucionalmente, bem como o aspecto de informações que foram coletadas e que possam ser publicadas, disseminadas em possíveis ataques cibernéticos que tratem de furto ou mesmo de vazamentos de dados e informações (EPM, 2020).

2.3.3 Como a LGPD aborda o tratamento de Dados Pessoais de Crianças e do Adolescentes

Inicialmente os dados pessoais que a LGPD menciona se refere a definição contida junto ao artigo 5º, I, que diz:

> Artigo 5º - Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável. (BRASIL, 2018)

Em decorrência no inciso X, traz o entendimento de que o tratamento de dados se refere a operação e classifica em 20 verbos que nada mais são do que ações que explicitam distintas maneiras de tratamentos de dados pessoais desses indivíduos.

Nesse cenário a lei incluiu diversos *direitos e deveres,* segundo os ditames do artigo 7°, da LGPD:

> Artigo 7º - O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de ***consentimento pelo titular;***
> II - para o cumprimento de ***obrigação legal*** ou regulatória pelo controlador;
> V - ***quando necessário para a execução de contrato*** ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
> VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

> IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.
> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.
> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores ***deverá obter consentimento específico do titular*** para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.
> § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.
> § 7º O tratamento posterior dos dados pessoais a que se referem os §§ 3º e 4º deste artigo poderá ser realizado para novas finalidades, desde que observados os ***propósitos legítimos e específicos*** para o novo tratamento e a ***preservação dos direitos do titular***, assim como os fundamentos e os princípios previstos nesta Lei. (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2018)

No caso do inciso II, a obrigação legal aqui deve ser entendida como aquelas a expensas dos provedores de *internet*, que possuem o dever de armazenar os registros digitais, bem como o cadastro das pessoas em decorrência da abrangência normativa e regulatória do Marco Civil da *Internet* (MCI) (EPM, 2020).

Em relação ao inciso V, a questão aqui pode ser interpretada segundo a necessidade de um estabelecimento escolar possuir os dados relativos a identificação de jovens (alunos), pois o tratamento ou a operacionalização desses dados deverão ser realizados sempre no melhor interesse do vulnerável (EPM, 2020).

Assim tudo que se refere a proteção de interesses individuais, claro objetivando as crianças e adolescentes deverão obviamente se sujeitar a tutela normativa, por isso dá importância da faixa etária do interessado, a fim de adoção de meios adequados como uma linguagem coloquial para também informar acerca dos riscos potenciais, aliado a informação de pais e responsáveis (EPM, 2020).

Portanto, é adequado dizer então que os termos de uso e as políticas de privacidade acerca dos serviços e produtos direcionados aos jovens devem estar

descritos de uma maneira de fácil entendimento, com clareza, simplicidade, precisão e de modo conciso (EPM, 2020).

Na LGPD existem alguns princípios que norteiam o tratamento de dados como, por exemplo, o *princípio da adequação* que aparece no contexto normativo quando os dados pessoais que foram coletados serão manipulados exatamente como foi anunciado a pessoa titular de direito. Já o princípio da necessidade se refere ao dado que foi apanhado é compatível com o serviço proposto (EPM, 2020).

O princípio da prevenção e não discriminação possuem o escopo de que os dados recolhidos não podem ser tratados com fins discriminatórios, ou mesmo ilícitos, com abuso, entre outras afrontas legais (EPM, 2020).

O artigo 18, da LGPD salienta como uma garantia de que as pessoas naturais titulares de seus dados podem exigir de controladores algumas providências como o ajuste de informações, ou seja, o ingresso aos dados que estejam inexatos, incompletos, bloqueados, desatualizados, bem como tratativas referentes ao compartilhamento desses dados e consequentemente o fornecimento ou não de seu consentimento que deve ser específico (concedido pelo responsável legal do menor) ou até sua revogação, inclusive questões relativas a anonimização e a eliminação de dados irrelevantes. Para as crianças o controlador deverá informar a utilização dos dados pessoais, tornando compreensíveis os procedimentos a serem realizados no exercício do direito (EPM, 2020).

Assim é óbvio que uma fotografia de um adolescente, por exemplo, disseminada via rede de *internet* e tornada pública interferirá na vida particular desse jovem envolvido. Esse fato se adequa perfeitamente ao foco de tutela legal ora estudada, especificamente no que tange ao tratamento de dados pessoais de sensibilidade extrema como uma imagem contendo um menor impúbere, levando em conta seu melhor interesse (EPM, 2020).

Considerando a ausência de consentimento do interessado apartado das regras previstas em lei, esse tratamento de dados pessoais será consagrado como de caráter ilícito, ofensivo, irregular e injusto, bem como sujeito as sanções legais, como também aliado a princípios que merecem o devido respeito e são afrontados, como o da transparência, que versa sobre o esclarecimento de dados consignados pelo controlador sobre a pessoa envolvida na coleta (EPM, 2020).

O artigo 52, da LGPD, implica na apresentação das punições vigentes pela violação às orientações da lei, como a submissão a advertência, bloqueio ou

eliminação de dados pessoais, multa simples ou diária de até 2 % do faturamento anual da pessoa jurídica ou grupo econômico no Brasil, com o limitador de 50 milhões de reais. As sanções possuem a faculdade de serem aplicadas de maneira paulatina, destacada ou até de forma associada a outras punições, sempre levando em consideração a gravidade da conduta, se houve ou não o instituto da boa-fé do autor, vantagens alcançadas, colaboração do transgressor, dentre outras (EPM, 2020).

2.3.4. A responsabilidade sob a ótica da LGPD

O escopo da LGPD visa a proteção, transparência e regulamentação acerca dos dados pessoais de cidadãos no país, abrangendo os âmbitos particulares e públicos (SOMADOSSI, 2018).

Como também todas as pessoas naturais ou mesmo as jurídicas de direito público ou privado, não importando a nação que estejam localizados, mas com alguns requisitos legais como a coleta e o tratamento de dados terem sido realizados no Brasil, a manipulação de dados tenha sido oriunda do fornecimento de bens (comércio em geral) ou serviços a brasileiros (EPM, 2020).

Mas a LGPD não será observada na ocasião de um propósito particular, sem intentos econômicos, acadêmicos, relativos a arte, editoriais/jornalísticos, como também aspectos relacionados à segurança pública, defesa nacional, segurança de Estado ou incumbências de caráter investigativo e/ou repressivo de condutas criminosas. Englobando os dados provenientes de estados estrangeiros e que sejam simplesmente processados em ambiente nacional, sem seu compartilhamento, comunicação ou disseminação dessas informações pelo intermediário brasileiro a outros colaboradores (EPM, 2020).

As empresas que oferecem entretenimento a crianças e adolescentes, por meio de aplicativos, sites, jogos e mídias sociais tratam informações pessoais, com base na coleta de dados de indivíduos usuários e obviamente necessitam se adequar às exigências normativas em vigor. É relevante salientar que estabelecimentos comerciais como hotéis, faculdades, fábricas, colégios dentre outros (EPM, 2020).

Claro que a seara escolar nesse estudo importa demasiadamente, pois através dela o cidadão em sua formação conquista a verdadeira cidadania,

sociabilidade e aprendizados diversos, incluindo a propensão ao mercado de trabalho, assim é indiscutível a carga positiva que o estabelecimento de ensino exerce nos jovens e sem dúvida nenhuma acrescenta tratativas educacionais de orientação no tocante ao uso correto, digno, eficiente, regular, justo e acima de tudo honesto das TIC (EPM, 2020).

Outra ideia salutar seria a implementação junto ao currículo escolar de crianças e adolescentes, de institutos importantes e modernos, que visam a aprendizagem *da proteção de dados e privacidade*, incorporando se necessário for a outras matérias escolares. O *tratamento de dados* também é outra modalidade necessária e valiosa, a fim de despertar a *compreensão/conscientização* dos envolvidos na problemática de dados pessoais junto as TIC (EPM, 2020).

Um bom exemplo, para um entendimento útil em relação a aplicação da LGPD na prática, aos jovens é das escolas particulares em que vigoram no caso de contrato de prestação de serviços educacionais em que há o tratamento de dados de pessoas menores (alunos), com alicerce nos princípios da minimização da colheita de dados, que significa apenas o estritamente necessário, como da finalidade e necessidade (EPM, 2020).

Dados em um outro momento de análise se referem ao compartilhamento de dados de alunos menores, que estão prestes a participarem de suas formaturas com a entidade organizadora do evento, sem o necessário assentimento, por mais simples e inofensivas que possam aparentar essas práticas, representam sim um abuso segundo os ditames da LGPD (EPM, 2020).

Argumentações que envolvam informações acerca de ordem étnica, genéticos, filosófica, biométrico, política, religiosa, cultural e orientação sexual não são justificativas plausíveis, para os estabelecimentos de ensino argumentarem que tais dados tem o condão de promover a agregação entre os alunos, pois a LGPD entende que determinados dados pessoais como estes são considerados sensíveis, portanto, há a concreta possibilidade de gerar ao portador da informação condutas desfavoráveis e discriminatórias, para o tratamento devem ser avaliados a efetiva necessidade os riscos, como a obtenção de consentimento particular (EPM, 2020).

A atuação escolar do aluno consequentemente é outro fator importante de análise, pois há a possibilidade de etiquetar, constatar o discente ou mesmo com a capacidade de torná-lo plenamente identificável, sob às óticas de outras situações acadêmicas, por exemplo, disciplina escolar, publicação em quadro dos alunos em

recuperação, sendo plenamente viável a postagem em local público do número de matrícula, homenageando assim a política da segurança da informação em ambiente escolar combinado com o progresso da educação digital no tratamento de dados pessoais (EPM, 2020).

2.4 Procedimentos Metodológicos

Com o objetivo de compreender a influência do instituto da Cidadania Digital na prevenção do *Ciberbullying* no *ciberespaço*, o estudo compreenderá um delineamento, por meio de uma abordagem qualitativa do tipo exploratória, revisão bibliográfica e documental, sendo os documentos de cunho primário, complementando com o respaldo do relatório de crimes cibernéticos da Norton, como também a legislação nacional que trata do instituto da proteção de dados e outras, incluindo a Constituição Federal de 1988, bem como a análise de todo esse arcabouço jurídico, as secundárias como artigos científicos, dissertações, framework da Unesco e livros, com o intuito de ancorar de maneira teórica e metodológica a análise de dados, conteúdo, objeto de pesquisa e discussão acadêmica.

As pesquisas qualitativas abarcam resultados de maneira verbal não alcançados pelos conhecidos procedimentos quantitativos aplicados, contudo, a diferença de ambos versa acerca de termos numéricos obtidos, que traduzem dados junto a pesquisa quantitativa, desencadeando a interpretação dessas informações, sob um enfoque positivista. Portanto, a pesquisa qualitativa nesse caso em comento, se traduz como sendo um importante instrumento de estudo abarcando o enigmático processo da interação social das comunidades, no uso regular das redes tecnologicamente mediadas, com base na utilização de rede de *internet* (GIL, 2019, p. 63).

A revisão de literatura se baseia em alguns eixos temáticos abordados, a Cidadania e Educação Digital, *Ciberbullying* e a Proteção e Privacidade de Dados, assim se define como sendo a prospecção, interpretação, apresentação, discussão dos materiais coletados, como os periódicos científicos, as dissertações, livros e conceitos que tratam especificamente do tema ora abordado, consubstanciando a necessária fundamentação teórica desse trabalho de pesquisa (GIL, 2019, p. 74).

A análise documental englobou legislações, o relatório da Norton, também as cartilhas que versam sobre temas atinentes ao Estatuto da Criança e do Adolescente (A Turma da Mônica no ECA), *Bullying* Não é Legal e Tolerância, cartilhas desenvolvidas pelo Ministério Público de São Paulo, bem como com o apoio do Centro de Apoio Operacional Cível e de Tutela Coletiva - Educação e a Associação Paulista do Ministério Público, ou seja, as fontes de consultas estão variadas.

Com relação a análise legislativa os documentos analisados nesta pesquisa foram a Constituição Federal de 1988, a Lei Geral de Proteção de Dados (LGPD) nº 13.709/18, Lei que institui o Programa de Combate a Intimidação Sistemática nº 13.185/2015 que está em vigor desde o dia 07 de fevereiro de 2016, o Marco Civil da *Internet* (MCI) - Lei nº 12.965/14, a Medida Provisória (MP) nº 869/18 e a Medida Provisória nº 959 de 29 de abril de 2020, que alterou alguns pontos da LGPD, inclusive sobre a *vacatio legis* e outros pontos.

Contudo a LGPD passou a vigorar no dia 18 de setembro de 2020, com a sanção da Lei nº 14.058/2020, que teve seu respaldo legal na Medida Provisória nº 959/20. Essa MP foi editada no mês de abril de 2020, sendo que o governo Jair Bolsonaro incluiu o artigo 4º, que trouxe o adiamento do início da vigência para maio de 2021, porém em análise conjunta realizada no Congresso Nacional esse dispositivo não foi aceito.

A seguir está demonstrado os procedimentos metodológicos, por meio do mapa mental abaixo exposto na Figura 3:

Figura 3 - Mapa Mental da Pesquisa

Fonte: Elaborado pelo Autor (2020).

O procedimento metodológico possibilita a seleção, acompanhamento, descrição e análise de casos que possuem elementos relevantes, para a pesquisa acadêmica, assim os desdobramentos da utilização da *internet* para a consecução e consumação do delito de *Ciberbullying* via rede de mundial de computadores no Brasil e no mundo.

A consecução também abarcará os cenários nos quais os criminosos se inseriram para a consumação dessas práticas delituosas, aliados aos cenários legislativos atuais, pois os crimes digitais são praticados em um contexto diferente dos delitos tradicionais e conduzem também a ofensa de bens jurídicos tutelados pela legislação de cunho criminal e outras vigentes no Brasil atualmente.

3 ANÁLISE E DISCUSSÃO DOS RESULTADOS

A tecnologia atual está indiscutivelmente presente no dia a dia das pessoas de 12 a 18 aos de idade e outras, com o uso frequente de e-mails, celulares, redes sociais, compras via site de *internet*, jogos *on line*, frequência em cursos via plataforma EAD, cultos religiosos *on line*, troca de informações em geral, redes de relacionamentos, admiradores de práticas relacionadas ao sexo virtual, enfim pesquisas diversas, relacionadas a trabalho ou mesmo estudos, mas o fato é que todos os indivíduos hoje estão conectados via rede de *internet*, seja em suas casas ou por meio de pacotes de dados de *internet* móvel.

Assim, é uma realidade que os indivíduos em locais distantes do mundo interajam ideias e pensamentos em curtíssimos espaços de tempo. Portanto, o modo de pensar, avaliar as coisas, obter informações e comunicar com pessoas mudou exponencialmente, especialmente em relação ao que tínhamos em termos de tecnologia no passado, não muito distante inclusive.

Tanto é que essa tecnologia repercutiu no seio do relacionamento entre os seres humanos, principalmente quando expressa poder, insatisfação, ódio, temor, sentidos, espaço, tempo e linguagens. Tecnologicamente há novas formas de ofender pessoas, expressar insatisfações, humilhar o outro com impropérios, riscar a imagem e reputação de outrem, praticar ameaças, condutas relacionadas a intolerância seja religiosa, sexual, étnica, de gênero, tudo via rede digital (ABRUSIO, 2015, p. 45).

O fato é que em tempos recentes ocorreram situações no Brasil e no mundo que despertam o intenso interesse público, os veículos jornalísticos dão grande destaque através de noticiários a esse tipo de informação, principalmente envolvendo o uso da rede de *internet*, para a consecução (tratativas) de empreitadas criminosas, sejam de ordem patrimonial como aconteceu na madrugada do dia 04 de abril de 2019, na pequena cidade de Guararema, localizada na Grande São Paulo, onde uma organização criminosa composta por 25 criminosos fortemente armados tinham o escopo de explodir duas agências bancárias, sendo uma delas o Banco do Brasil (BB) e a outra do Santander, a fim de obterem grandes vantagens patrimoniais (dinheiro em espécie) ilícitas.

Em outra vertente na cidade de Suzano/SP, na manhã do dia 13 de março de 2019, dois rapazes (um de 17 e outro de 25 anos), ex-alunos do estabelecimento

de ensino, invadiram a Escola Municipal Professor Raul Brasil e brutalmente assassinaram pessoas (alunos, professores e funcionários da escola) desnecessariamente e que ali estavam na ocasião do delito, frequentando normalmente as aulas ou mesmo as atividades relacionadas ao expediente de trabalho, porém tudo em ambiente escolar no momento da carnificina.

Mas o cerne da questão denota que as tratativas para a consecução desse delito bizarro aconteceram via rede de *internet*, desde a aquisição das armas de fogo (tipo e porte), munições (quantidades), escolha do estabelecimento de ensino (alvo), planejamento das ações de entrada no prédio da escola (por qual porta será a escalada criminosa), assim se percebe o nível das negociações que ocorreram antes dos fatos se consumarem via rede.

Outra situação lamentável ocorreu no domingo dia 17 de março de 2019, na cidade de *Christchurch*, na Nova Zelândia, mais especificamente em frente à Mesquita Al Noor, onde um indivíduo de nome Brenton Tarrant, de origem australiana estacionou seu veículo marca Subaru do outro lado da via pública, desceu e foi até o porta malas do veículo automotor, consequentemente retirou seu armamento longo que carregava e que na verdade se tratou de uma metralhadora semi automática modelo AR-15 utilizada no massacre.

Brenton caminhou em direção da porta de entrada da mesquita e em seguida disparou contra a primeira pessoa que infelizmente estava próxima ao acesso, sendo que toda a ação foi filmada e transmitida de maneira *on line* via rede social *Facebook* (RODRIGUES, 2019).

Outro aspecto importante trata dos artigos pesquisados no site *Web Of Science*, um deles é o *Offending and Victimization in the Digital Age: Comparing Correlates of Cybercrime and Traditional Offending-Only, Victimization-Only and the Victimization-Offending Overlap* (WEULEN KRANENBARG *et al*., 2019), que traz uma temática relacionada fortemente ao empirismo em um contexto de amostras de alto risco de *ciber* criminosos dependentes de computadores e criminosos tradicionais, comparando-se a vitimização infratora entre a *ciber* criminalidade e a tradicional.

> Também o artigo *Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates*, de um pesquisador norte americano, relaciona demasiadamente os vários crimes digitais com o PIB (produto interno bruto) dos países mais ricos do mundo (KIGERL, 2016).

No entanto, Stratton *et al*. (2017) mencionam com propriedade acerca de uma nova modalidade criminosa digital que ainda não é conhecida no Brasil, trata-se do *ciberstalking*, uma espécie de *ciberviolência*, como também o *ciberterrorismo* e o extremismo *on line*, se mostrando inclusive um grande desafio para as legislações futuras a respeito desse assunto no Brasil.

Pinheiro (2019) expôs uma realidade preocupante para o cenário nacional, trazendo a informação de que os Estados Brasileiros que apresentam maior concentração de *cibercriminosos* são Goiás, Pará, Maranhão e Ceará, bem como para o crescimento demasiado das práticas de crimes virtuais no país, principalmente as relacionadas com à fraude bancária, comercialização de dados via *deep* e *dark web* e que ambas são acessadas por meio do navegador conhecido como TOR.

No Brasil existem obstáculos legais e estruturais que na verdade são entraves para o combate efetivo dessas modalidades delituosas existentes hoje no país e mundialmente. Assim, como existem no mundo todo, países que são considerados *"paraísos fiscais"*, o Brasil infelizmente está se tornando um *"paraíso digital"*, em virtude dessas pessoas encontrarem um ambiente propício, para o desenvolvimento de seus atos criminosos (PINHEIRO, 2019).

Um exemplo concreto desse caótico cenário versa sobre um israelense de nome *Tal Prihar* de 37 anos, que mantinha uma vida confortável e discreta junto à sua esposa e 4 filhos em uma bonita casa localizada no Lago Sul, quadra nº 22 de Brasília/DF, mas o fato é que esse indivíduo coordenou e intermediou mais de 40 mil transações ilícitas de armas, lavagem de dinheiro, drogas e material de pornografia infantil diretamente de um local estratégico, ou seja, próximo a várias embaixadas e do Aeroporto Internacional de Brasília/DF, portanto, o israelense escolheu a região administrativa mais segura da Capital Federal, bem como se percebe que houve por parte dessa pessoa um planejamento prévio em relação a escolha do local, para viver tranquilamente com seus familiares e para colocar em prática suas empreitadas delitivas via plataforma *on line* (PINHEIRO, 2019).

Ainda, *Tal Prihar* e outros israelenses operavam desde o ano de 2013 no Brasil, administrando um site conhecido como ***deepdotweb.com***, uma verdadeira ameaça global, consequentemente a atividade clandestina permitiu que *Prihar* acumulasse um montante de US$ 15 milhões em *criptomoedas*. *Tal Prihar* foi identificado e investigado, por meio de uma cooperação conjunta de âmbito internacional entre as polícias dos EUA e do Brasil, como também foi preso na cidade de Paris no dia 06 de maio de 2019 (PINHEIRO, 2019).

Outro aspecto interessante segundo o Olhar Digital (2019), se refere a resposta de uma nação fortemente militarizada a um *ciberataque*, mobilizando suas forças militares nacionais ocorrido no início de maio de 2019, para uma forte empreitada contra um ataque cibernético alimentado através do site ***hamascyberhq.exe***, sendo a primeira ação militar conhecida na história com essa finalidade em específico. Essa situação ocorreu na Faixa de Gaza/Palestina, mais especificamente em um prédio que servia de base da inteligência militar e atuação do Hamas, para um grupo de *hackers* e *crackers*, ocasionando a morte de 25 pessoas que se encontravam presentes no momento do destrutivo ataque israelense.

Essa realidade segundo o Minuto da Segurança (2019) é conhecida como *guerra híbrida*, pois se trata de um misto entre o espaço *ciber* e físico, inclusive com a mobilização de tropas militares em ações específicas de combate, como as usadas pela IDF – Força de Defesa de Israel associadas a utilização de *drones*, incluindo atos de vigilância e ataques com alvos identificados.

Outro aspecto relevante se relaciona aos dados pessoais de clientes de uma grande rede mundial de hotéis denominada Marriott, que atua em cerca de 110 países e possui 5 mil propriedades espalhadas pelo mundo, pois uma falha na segurança afetou todo o sistema de reservas do hotel (conhecido por *starwood)* e que pode ter afetado cerca de 500 milhões de pessoas, em virtude da ação de hackers junto ao banco de dados da empresa, assim em decorrência desse ataque informações como nomes, números de telefones, cartões de crédito, inclusive com as respectivas datas de vencimentos, endereços de e-mail, números de passaportes, datas de nascimentos e dados de chegadas e saídas foram todos devassados, isso a partir de 2014, com a descoberta apenas sendo realizada ao final de 2018, assim os cidadãos afetados permaneceram por 4 anos sem uma

providência efetiva por parte das autoridades competentes (JORNAL GLOBO, 2018).

Da mesma forma aconteceu no dia 11 de abril de 2019, com o Sistema Único de Saúde (SUS) brasileiro, em que 2,4 milhões de indivíduos tiveram seus dados pessoais *expostos/devassados*, que estavam alocados em um banco de dados, como nomes dos titulares, de suas genitoras, endereços, CPF e datas de nascimentos de cidadãos cadastrados no serviço foram completamente vulnerabilizados (SILVA, 2019).

A ação contra o SUS foi reivindicada pelo autor denominado *"Tr3v0r"*, que afirma ter reunido cerca de 205 milhões de dados pessoais que estavam em posse do SUS. A brecha estaria em uma API (conjunto de rotinas e padrões de programação), que permite consultar dados de usuários do sistema único de saúde, a partir do número do cartão do serviço e uma senha (SILVA, 2019).

Ademais em um site do BB Previdência trouxe a exposição de cerca de 153 mil clientes junto a plataforma, que além dos dados pessoais, campos editáveis para a realização de transferências de recursos inclusive a qualquer beneficiário, portanto, uma manifestação explícita de falha da segurança cibernética da empresa e que não exigia conhecimento avançado algum em matéria de programação, a fim de obtenção de dados de terceiros (clientes), bastava possuir o link de acesso da conta BB Previdência, incluindo os clientes do serviço e utilizar o mesmo endereço eletrônico e substituir aleatoriamente o "número sequencial do participante" o qual aparece ao final do endereço (NAKAGAWA, 2020).

Interessante, que o mais grave é que o ambiente digital possui a certificação HTTPS e ainda permite a edição de *dados/informações* incluindo a inclusão de terceiros e a exclusão de indivíduos cadastrados na plataforma, no exemplo do Banco do Brasil (BB) que reconheceu a fragilidade junto ao sistema de previdência e suas funcionalidades retirou a página do ar (retirado de patrocínio) com o intuito de subsidiar medidas de identificação e correção para salvaguardar o perfeito sigilo de *dados/informações* de clientes (NAKAGAWA, 2020).

Com relação ao termo *Ciberbullying* objeto dessa pesquisa científica, por exemplo, utilizado repetidamente e intencionalmente com o intuito de proferir atos de violência contra outro ser humano, utilizado muito, por meio das plataformas de tecnologia da informação e comunicação dispostas em sites eletrônicos, blogs,

celulares, grupos de discussão e redes sociais, são também práticas bem conhecidas no Brasil (ABRUSIO, 2015, p. 82).

A Lei nº 13.185/2015, que trata do Programa de Combate à Intimidação Sistemática conhecida como *bullying*, em seu artigo 1º, parágrafo 1º, considera como intimidação sistemática, portanto, *bullying:*

> § 1º - todo ato de violência física ou psicológica, intencional e repetitivo que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio de poder entre as partes envolvidas (BRASIL, 2015).

A prática de *Ciberbullying*, por sua vez desencadeia a insistente constrangimento, embaraço junto à rede mundial de computadores, sendo que nesse caso são utilizados os meios próprios da *internet* para atacar o jovem com ações depreciativas, violentas, bem como a ocorrência de exibição de fotos *alteradas/deturpadas*, mas possibilitando a identificação do menor impúbere vítima da prática delitiva (BARRETO; ARAÚJO, 2017).

A conduta do envio de fotos e vídeos conhecidos hoje por *nudes* via plataformas de TIC, são hábitos costumeiros entre o público jovem e adolescente, portanto, esse modelo de namoro virtual que carrega um grande volume de material erótico que foi disseminado como as exposições pornográficas não consensuais, pode ocasionar uma enorme devassa na vida privada, incluído a escolar da vítima, pois se propagar junto as plataformas digitais causará a manifestação em massa desse conteúdo (BARRETO; ARAÚJO, 2017).

A sanção social em desfavor desse público jovem, infelizmente são enérgicas, severas e doloridas, pois no caso de meninas podem gerar até perseguições em estabelecimento escolar, em locais públicos como em ruas, círculos sociais e que muitas das vezes essas vítimas até excluem suas vidas, em virtude do imenso sofrimento, como pela vergonha que causaram em suas famílias. Contudo o indivíduo responsável por essa prática cruel tem a óbvia intenção de deteriorar a imagem, privacidade e intimidade, com o escopo de causar um profundo sofrimento e a infâmia pública ao menor (BARRETO; ARAÚJO, 2017).

Assim o legislador brasileiro atento a essa nova modalidade criminosa que atinge principalmente o público jovem de 12 a 18 anos, trouxe na forma de uma lei, o

Programa de Combate à Intimidação Sistemática conhecida como *bullying*, cujo escopo versa sobre a promoção de um cenário de paz, tranquilidade, equilíbrio, empatia aos adolescentes, levando em conta a conscientização, capacitação de docentes, campanhas de educação, informação, orientação aos pais, familiares, assistência psicológica, dentre outros, em detrimento da efetiva prevenção e combate aos tipos de violência existentes hoje, mais especificamente com relação ao contexto do *bullying* (BARRETO; ARAÚJO, 2017).

Tratando de legislação brasileira pertinente a Lei do Marco Civil da Internet nº 12.965/14, por sua vez disciplina o uso da *internet* no país e apresentam como princípios a liberdade de expressão, comunicação, manifestação de pensamento, assim como na Constituição Federal de 1988 e a proteção da privacidade, dos dados pessoais, nos termos do artigo 3º, da lei. Assim o Marco Civil da *Internet* (MCI) tem como objetivo o direito ao acesso à rede a todas as pessoas, o acesso à informação e ao conhecimento, conforme preceitua o artigo 4º, II (BRASIL, 2014).

Contudo, o artigo 7º, do MCI disciplina que acessar a *internet* é essencial ao exercício da cidadania das pessoas, portanto, ao indivíduo usuário da rede está assegurado o direito da inviolabilidade da intimidade, da vida privada, a proteção e indenização pelo dano material e/ou moral decorrente dessa violação (BRASIL, 2014).

O inciso VIII, do artigo 7º do MCI, menciona que:

> O não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de *internet*, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (BRASIL, 2014).

Ademais, o MCI é considerado a *Constituição da Internet*. Traz uma *carta de princípios*, direitos e deveres dos usuários da rede de *internet*, dos portais e sites, das prestadoras de serviço e do Estado (PIMENTEL, 2018).

Pimentel (2018) entende também que embora o MCI tutele direitos de cunho civis junto a rede de *internet*, há uma extensa aplicabilidade no Direito Penal e Processual Penal, pois estabelece conceitos fundamentais que disciplinam a obtenção de provas concernentes à materialidade delitiva e a autoria criminosa.

O MCI traz ainda sanções de advertência, multa de até 10% do faturamento do grupo econômico no Brasil, suspensão temporária das atividades, proibição de

exercício das atividades e se tratando de empresa estrangeira responderá solidariamente pelo pagamento da multa de sua filial, escritório, sucursal ou estabelecimento situado no país, segundo dispõe o artigo 12 e incisos (BRASIL, 2014).

A Lei Geral de Proteção de Dados nº 13.709/18, sancionada pelo Presidente da República no dia 14 de agosto de 2018, entrou em vigor na data de 18 de setembro de 2020, conhecida popularmente como LGPD, traz sua aplicação a qualquer pessoa, seja natural ou jurídica de direito público ou privado, que realize o tratamento de dados pessoais seja de maneira *on line* ou mesmo *off line* (FIESP, 2018).

A LGPD possui aplicação extraterritorial visando empresas que não tenham estabelecimento instituído formalmente no Brasil, mas que ofereçam serviços e produtos no mercado consumidor brasileiro ou que coletem e tratem de dados de indivíduos localizados no país, que são na verdade são consumidores. O objetivo da LGPD é de proporcionar proteção aos direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa humana, bem como identificar regras e limites para as coletas/tratamentos dos dados e informações de cunho pessoal (FIESP, 2018).

As empresas de todos os setores e de todos os portes são obrigadas a tratar os dados pessoais, assim à lei se aplica e vale para as empresas, bem como atender os princípios da finalidade (propósitos legítimos), para o tratamento de dados, adequação (compatibilidade), necessidade (mínima coleta) e transparência (FIESP, 2018).

Houve também a criação da figura da Autoridade Nacional de Proteção de Dados (ANPD), órgão ligado à Presidência da República e o Conselho Nacional de Proteção de Dados Pessoais (composto por 23 representantes), a fim de fiscalizar o cumprimento da legislação, aplicar sanções (competência exclusiva da ANPD), como multa que poderá chegar ao patamar de 50 milhões de reais e editar normas e procedimentos em relação as tratativas sobre a questão envolvendo dados pessoais (FIESP, 2018).

O dado pessoal está definido no artigo 5º, I, da LGPD, que salienta que é informação relacionada a pessoa natural identificada ou identificável, como por exemplo, dados cadastrais, profissão, hábitos de consumo e dados de GPS. Em contrapartida há o dado pessoal sensível, segundo o artigo 5º, II, é aquele que versa

sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou a vida sexual, dado genético ou biométrico (FIESP, 2018).

Existe a figura do dado anonimizado, conforme preleciona o artigo 5º, III, do mesmo diploma legal, é relativo então ao titular que não possa ser identificado e se mostra primordial o uso desses dados, a fim de possibilitar o desenvolvimento e aprimoramento de novas tecnologias como a *internet* das coisas e a inteligência artificial. Outra importante menção que a LGPD trouxe diz respeito aos documentos confidenciais, segredos de negócios, fórmulas, algoritmos, direitos autorais ou propriedade industrial e que não serão objetos de atribuição da LGPD (FIESP, 2018).

Tratamento de dados pessoais, portanto, nos termos do artigo 5º, X, se resume a toda operação realizada com dados pessoais, que na verdade são 20 verbos/ações que vão desde uma simples coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, até a difusão ou extração do dado pessoal (FIESP, 2018).

No tocante, a base legal para o tratamento de dados pessoais, há a necessidade de consentimento do cidadão, titular dos dados, com sua manifestação inequívoca, livre e informada, para uma finalidade específica de tratamento, seja para exercer a defesa de direitos em processo judicial administrativo, segundo a leitura do artigo 7º, da lei, assim consequentemente quem trata dados pessoais devem se respaldar em um dos incisos como fundamento legal (FIESP, 2018).

Sobre a Medida Provisória nº 869/18 foi editada em 27 de dezembro de 2018, trouxe algumas modificações na LGPD, como a revogação de alguns dispositivos da lei e sacramentou a criação da Autoridade Nacional de Proteção de Dados (ANPD), com autonomia técnica, sendo os membros nomeados pelo Presidente da República.

Assim o prazo legal da *“vacatio legis”* da LGPD foi estendido de 18 meses para 24 meses e agora por mais alguns meses, portanto, previsto então para maio de 2021, com nítido intuito de adaptação e adequação à lei pelos sujeitos envolvidos no contexto referente ao tratamento de dados pessoais.

Na Câmara do Deputados a LGPD foi aprovada no dia 28 de maio e no Senado Federal no dia 29 de maio de 2019, recentemente e já com as alterações, o texto final modificado foi sancionado em agosto de 2018. A Lei nº 13.853 de 08 de julho de 2019 se originou da aprovação da Medida Provisória nº 869/18, com a alteração de alguns dispositivos da Lei nº 13.709 (LGPD).

Em outra trajetória, a Educação Digital funciona como um instituto importante na atual conjuntura do uso frequente das plataformas tecnológicas digitais pelas pessoas nesse Brasil de dimensão continental, mas depende inevitavelmente de *políticas públicas* contundentes/eficientes e nesse contexto também de como serão desenvolvidas e difundidas, com um sério e comprometido planejamento prévio, aliado à eficácia na implementação e gestão dos recursos estatais ora destinados (CORDEIRO; BONILLA, 2018).

As políticas públicas se definem como sendo um conjunto integrado de princípios de atuação, relacionadas a atividades de comunicação. Orientam processos de interação consubstanciados em trocas de informações de interesse coletivo, induzindo a participação em debates e ocasionando a institucionalização do atendimento do interesse público junto aos cidadãos (DUARTE, 2007).

O fato é que projetos direcionaram para distribuição da rede de *internet* nas escolas públicas brasileiras, por meio de alguns programas governamentais como Proinfo, Proinfo Integrado, Banda Larga nas Escolas, Um Computador por Aluno, Programa de Implementação de salas de Recursos Multifuncionais, Programa Gesac e segundo dados da ANATEL 2014, nos anos de 2008 a 2010 durante o governo Lula houve uma alavancagem no atendimento, cumprindo a meta de instalação da rede em 76% do número de escolas (CORDEIRO; BONILLA, 2018).

Nos governos seguintes, ou seja, Presidentes Dilma e Temer, os programas não foram adiante, menos ainda no mesmo ritmo e por vários motivos entre eles a alteração de interesses dos gestores envolvidos na temática. Outro problema relevante que ficou evidenciado com a intenção de propiciar conectividade nas escolas foi a qualidade da conexão da rede de *internet*, a velocidade se mostrou precária e incompatível com a real necessidade do aprendizado digital requer, por isso há necessidade de investimento estatal, por meio de políticas públicas eficientes (CORDEIRO; BONILLA, 2018).

Assim não basta conectar à rede, mas sim perceber a qualidade final dessa conexão, pois se dessa maneira não o for, não há possibilidades no campo das

estratégias em disponibilizar as pessoas a troca saudável de informações junto à rede e a disseminação do conhecimento cultural necessário que a Educação Digital proporcionará em nível social no país, o que demonstra que a baixa conectividade é uma questão de carência relacionada a infraestrutura e sustentabilidade governamental (CORDEIRO; BONILLA, 2018).

Esses ensinamentos digitais são essenciais para a boa manutenção da ordem pública no Brasil, nos termos do artigo 144, da Constituição Federal de 1988 (BRASIL, 1988), porque o cidadão de bem somente terá o conhecimento necessário e real sobre os aspectos de segurança da informação com uma orientação educacional digital elevada, direcionada, pois os crimes cometidos em ambiente cibernético, obviamente afrontam também os bens jurídicos tutelados pelo Estado, como o patrimônio, a privacidade de dados pessoais, a vida, a honra, a imagem, delitos de ódio, intolerância racial ou étnica, religiosa, sexual, política, de gênero, crimes contra a incolumidade das pessoas, enfim trazem a mesma sensação de insegurança pública que há no cotidiano físico/real das pessoas e a tendência infelizmente é de aumento.

Aliado ao fato das legislações abordadas nessa temática, tratarem de que a proteção de dados tem como um de seus fundamentos, segundo o artigo 2º, VII, da LGPD os direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018). Questão que inclusive envolve um princípio de ordem constitucional conhecido como um *super princípio*, o da *dignidade da pessoa humana*, reconhecido como um dos pilares fundamentais da República Federativa do Brasil elencado junto ao artigo 1º, da Constituição Federal (BRASIL, 1988).

Então a busca de conhecimento e informação através da rede de *internet,* conforme menciona o artigo 7º, do Marco Civil é essencial ao pleno exercício da cidadania e a garantia do direito à privacidade é uma das condições para o pleno exercício do direito de acesso à *internet* (BRASIL, 2014). O MCI consequentemente descreve que ao utilizar a rede de *internet,* se trata então da busca pelo conhecimento e informação, isso nada mais é do que exercer a cidadania em sua plenitude e exercê-la é, portanto, um direito que leva a ter dignidade da pessoa humana, a ter seus dados pessoais tutelados pelo Estado, que inclusive se torna o garantidor da ordem pública.

Por fim, o artigo 26, da MCI afirma que:

> o cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, **inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da *internet* como ferramenta para o exercício da cidadania,** a promoção da cultura e o desenvolvimento tecnológico (BRASIL, 2014).

O instituto da Cidadania Digital na Prevenção dos *Ciberbullying* deverá ser compreendido como um dever de Estado, podendo ser condicionado, por meio de políticas públicas contundentes e eficientes, um direito e responsabilidade de todos os cidadãos, sejam oriundos da sociedade civil, governo, instituições de ensino, pais, provedores de conexão e de aplicação, pois quando o indivíduo busca informação e conhecimento junto a rede de internet exerce também sua cidadania (MIGALHAS, 2019).

Assim essa pesquisa contribui primariamente para o desenvolvimento de boas práticas no uso das plataformas digitais (TIC), por meio dos institutos da Cidadania e Educação Digitais, como também pela aplicação dos ditames contidos na Lei nº 13.185/2015, que trata do Programa de Combate à Intimidação Sistemática conhecida como *bullying,* combinada com o Marco Civil da *Internet,* ainda com as tratativas implementadas pela LGPD no ordenamento jurídico pátrio e aliadas aos documentos da UNICEF, UNESCO, *SAFERNET* e as Cartilhas, bem como pelas orientações dos responsáveis por esse público jovem, fará a esperada identificação e prevenção da prática do *Ciberbullying*.

No tocante ao aspecto das medidas técnicas mencionadas no objetivo principal desse trabalho, são aquelas que protegem os dados pessoais aliadas às condições de segurança da informação e comunicação nas plataformas TIC, o bom senso e o respeito digital, aliadas a medidas de *compliance*, por exemplo, que são ações que visam e buscam padrões éticos e morais elevados.

As relações *on line* devem seguir sempre os mesmos parâmetros das presenciais, que vão desde a atenção à escrita gramatical em uma rede social até a moderação em postagens contendo informações de cunho pessoal principalmente, pois assim, poderá ocorrer a exposição exacerbada do indivíduo e com isso advir consequências indesejadas para o autor.

Claro que a ausência dos institutos da Cidadania e Educação Digital proporciona reflexos expressivos no campo da segurança pública brasileira, pois notadamente suas finalidades são a preparação de jovens para uma sociedade

direcionada às plataformas TIC, que são inclusive muito presentes na vida dessa classe, de uma maneira segura, eficiente e sempre abordando a seara do respeito e do bom senso virtual.

Os jovens possuem a realidade de uma efetividade de integração com o mundo contemporâneo e desse mundo atual com esses indivíduos alvo desta pesquisa, pois assim há a possibilidade de conhecer as reais ameaças digitais, suas potencialidades de risco e avaliar as oportunidades que surgem nesse cenário cibernético.

No entanto, de maneira secundária houve a proposta de um Folheto Digital com foco no público alvo referente a jovens e adolescentes com idades entre 12 a 18 anos de idade, tratando de aspectos sobre a identificação e prevenção da conduta criminosa de *Ciberbullying*.

Assim diante da pergunta problema que alcançou a resposta contida no bojo deste trabalho, bem como os objetivos principal e secundário, este então com a proposta de folheto digital.

Por fim, aliado ao fato de um combate efetivo ao desvio de conduta das pessoas em todos os níveis existentes na sociedade contemporânea, como acontecem nas empresas, instituições e órgãos públicos e privados ao redor do mundo, pois a cultura da corrupção e da coisa fácil denota a crise ética e moral atual em variados níveis e setores da vida cotidiana no Brasil, que ao final sempre atingem de frente o bem estar do cidadão, por inúmeros aspectos sejam econômicos (aumento de impostos), sociais (serviço de péssima qualidade *prestado/oferecido* pelo Estado), profissionais (condutas antiprofissionais em ambiente de trabalho), pessoais (figurar como réu em processo crime de corrupção), familiares (desestruturação das famílias), assim em momentos como o vivenciado há necessidade de reflexão no campo da ética, moral, da integridade, idoneidade, com o escopo de restauração social dos seres humanos, a fim de atingir a paz social.

4 ESPECIFICAÇÃO DA PROPOSTA DE INTERVENÇÃO OU APLICAÇÃO

Com relação à proposta de intervenção, considerar o produto a proposta de folheto em formato digital, elaborada por um profissional na edição de desenhos e que retrate aspectos de conhecimento e prevenção do crime cibernético conhecido como *Ciberbullying* e que verse sobre a importância da segurança pessoal de jovens e adolescentes na faixa etária entre 12 a 18 anos de idade, no tocante a essa perversa prática, que infelizmente com a TIC cresce de forma exponencial.

As tratativas serão direcionadas para o instituto da Cidadania Digital, com o escopo principalmente no desenvolvimento de boas práticas no uso de plataformas digitais, como também voltado e focado em uma abordagem técnica de boas práticas digitais.

O folheto foi desenvolvido como uma ferramenta de marketing direcionada a publicidade educacional e de cidadania, pois apresenta um conteúdo bem direcionado, na qual a pessoa que lê, pode ou não se identificar com a conduta delitiva descrita e saber que aquilo que está sofrendo, se trata de um constrangimento, que na verdade é nocivo e necessita de ajuda de pessoas confiáveis.

Este trabalho faz menção, pois abrange recomendações, dicas e benefícios direcionados ao usuário da rede, assim como se comportar diante de um cenário de *ameaças/ataques* e práticas criminosas consumadas, tudo com o intuito de aumentar a segurança e proteção de riscos, pois o principal intuito desse trabalho será de esclarecer que na verdade não há nada de virtual e que os cuidados a serem tomados deverão ser semelhantes aos que propiciamos em nossas atividades cotidianas.

4.1 Exemplos exitosos de Cartilhas em prol da Cidadania Digital

Existe o Estatuto da Criança e do Adolescente – ECA (A Turma da Mônica no ECA), *Bullying* Não é Legal e Tolerância, cartilhas estas desenvolvidas pelo Ministério Público do Estado de São Paulo e a última com a colaboração do Centro de Apoio Operacional Cível e de Tutela Coletiva - Educação e a Associação Paulista do Ministério Público.

Figura 4 - A Turma da Mônica no ECA

Fonte: SOUZA (2006).

A cartilha da Mônica, por exemplo, retrata a exposição do ECA, por meio de história em quadrinhos vivenciada pelos personagens – grupos de amigos amplamente conhecidos no mundo animado da Turma da Mônica. Ainda o prospecto educacional menciona a respeito das garantias legais da criança, como direito a vida, alimentação, nascimento com um desenvolvimento sadio, atendimento médico e odontológico, respeito, a liberdade, cultura, religião, de brincar, praticar esportes e diversão (SOUZA, 2006).

Contudo, para o adolescente ao completarem 16 anos de idade há a possibilidade de participação na política, ao exercer o seu direito de voto, inclusive é dever de todos proteger a criança e adolescente do tratamento desumano e violento. O ECA concede a esse público o direito à liberdade de expressão, de trabalho, de ser criado e educado pela sua família e trata do assunto concernente a adoção e do Conselho Tutelar (SOUZA, 2006).

Com relação à rede de *internet* a cartilha menciona que a supervisão do uso regular seja realizada pelos pais ou responsáveis. A cartilha *Bullying* Não é Legal trata mais especificamente do *bullying*, discorrendo aspectos importantes sobre autores, vítimas, características dessa conduta, o papel da escola, da família e do

sistema de garantias dos direitos da criança e dos adolescentes que pertence ao Ministério Público (MPSP, 2010).

Figura 5 - *Bullying* Não é Legal

Fonte: MPSP (2010).

Versa também sobre a velocidade das informações veiculadas em redes sociais e do anonimato ou nomes falsos, nas quais o agressor pode se beneficiar aliado a cuidados com a exposição pessoal, como a divulgação de endereço, e-mail, telefones, compartilhamento de fotos, vídeos e alerta para o público que se expõe demais na rede, poderá ser alvo de ataques maldosos e ofensas diversas (MPSP, 2010).

Já a edição Tolerância desenvolvida também pelo Ministério Público do Estado de São Paulo exalta a dignidade da pessoa humana, a igualdade entre homens, mulheres, crianças, idosos e indivíduos com todas as suas características e opções pessoais, como também a Declaração Universal dos Direitos do Homem em seus artigos I e II (MPSP, 2016).

Figura 6 - Edição Tolerância

Fonte: MPSP (2016).

Discorre sobre a igualdade, que para a lei brasileira se trata de uma forma de garantia a todas as pessoas aos mesmos direitos, ainda que esses indivíduos sejam diferentes. O objetivo da Constituição Brasileira de 1988 é a promoção do bem geral, de todos, portanto, sem preconceitos, seja de origem, raça, sexo, cor, idade ou quaisquer maneiras distintas de discriminação (MPSP, 2016).

Mas ainda que haja diferenças, em contextos de pensamentos, manifestação e ação é exatamente nessa situação de diferenças, que o respeito deverá emergir e propagar a convivência pacífica. Assim a palavra tolerar é respeitar o seu próximo, mesmo que seja um indivíduo desconhecido, demonstrando assim com essa conduta que apesar de pensar e agir diferente de você ele não é seu inimigo, dessa forma significa aceitar pacificamente a opinião alheia (MPSP, 2016).

Os tentáculos da intolerância levam com toda a certeza ao preconceito seja de qual ordem for, racial, de gênero, econômico, sexual, social, de pessoa portadora de deficiência, religioso, esportivo, etário e político. A tolerância está intrinsicamente

relacionada com a ética da reciprocidade, que possui como escopo o tratamento destinado a outrem de como gostaria de ser tratado (MPSP, 2016).

A crítica é um direito respaldado constitucionalmente ao cidadão na seara das liberdades de opinião e expressão, contudo, devem assumir um papel civilizado sem menções a declarações de ódio e desrespeito a terceiros, a intolerância incentiva contendas e demanda ódio (MPSP, 2016).

As redes sociais atualmente existem indivíduos que procuram muitas vezes manifestar comportamentos, condutas que no dia a dia procurariam omitir, esconder, ofuscar, pois se tratam de questões de grave ordem (MPSP, 2016).

O caminho eficaz para combater a intolerância é pela via educacional, cultural, trazendo para esse público elevados padrões de ética e moral dessas pessoas (MPSP, 2016).

4.2 Método utilizado para o Produto Final

O método de pesquisa a ser utilizado na elaboração desse produto profissional se refere a técnica conhecida como *Design Thinking*, desenvolvida como sendo um fomento para cenários de inovação em relação a produtos e serviços, pois adequa como benéfico a maneira de *pensar e trabalhar designers* e ideias (TSCHIMMEL, 2012).

Se trata então de uma forma de pensar que visa a busca e a transformação, a inovação e consequentemente a evolução, portanto, concentrada especificamente no ser humano. O *Design Thinking* é um método acentuado de pensamento, uma verdadeira caixa de ferramentas destinada a qualquer processo, que visa a busca do conhecimento de outras realidades na seara da inovação (TSCHIMMEL, 2012).

Outro aspecto relevante a ser considerado aqui é que o *Design Thinking*, que ressalta ser uma abordagem apartada de conceitos formais, funcionais ou mesmo estéticos. Nas aplicações dessa técnica há necessidade de se pensar, por meio de uma experiência própria, que moldura o problema e diante desse cenário, busca meios adequados e criativos que gere soluções factíveis (STICKDORN; SCHNEIDER, 2014).

Nesse caso em comento o *Design Thinking* auxiliará no desenvolvimento de uma necessidade humana concreta de determinado grupo de pessoas vulneráveis que são tuteladas pela legislação pátria, ou seja, crianças e adolescentes entre 12 e

18 anos de idade, no uso frequente da rede de *internet*, por meio das plataformas digitais de informação e comunicação (TSCHIMMEL, 2012).

O desenvolvimento da proposta de um folheto digital foi pensado (visualização de pensamentos) e desenhado, por meio de um esboço em um papel A4 (sulfite) em branco, que explora o cenário atual de um *cibercrime*, amplamente conhecido como *Ciberbullying.* Assim as ideias apareceram e aplicadas em um processo de design, surgiu daí a interação com o papel em branco quando explicitado por uma representação externa, articulando um diálogo agradável entre a problemática e o produto final.

Portanto, este folheto digital se resume a um material de comunicação e informação, portanto, uma ferramenta de marketing direcionado a uma publicidade adequada, ou mesmo disseminando conteúdos de cunho educacional, como neste caso, trazendo uma boa qualidade e facilidade de leitura para o público alvo, podendo ser apresentado tanto em formato A4 ou A5.

Essa metodologia *Design Thinking* é prazerosa, porque o apoio mental que a visualização fornece conciliada com o aspecto lúdico do esboço aliado ao desenho propriamente dito trazem algumas respostas seguras, no trato com o produto da dissertação. A maneira visual de uma ideia em um protótipo testável busca indiscutivelmente o processo de design criativo e mais ainda concede o benevolente efeito do erro (TSCHIMMEL, 2012).

4.3 Proposta de Folheto Digital

Dessa forma, a proposta de elaboração do folheto digital está disposta no Quadro a seguir:

Quadro 2 - Proposta de Produto Profissional da Dissertação

Público Alvo	Crianças e Adolescentes de 12 a 18 anos de idade
Objeto	Elaboração de um Folheto na Forma Digital
Tema	Prevenção da Prática de *Ciberbullying*
Layout	Divisão em 3 (três) partes de um sulfite em branco A4 excluindo o cabeçalho
Ideia de elaboração	Contratação de um profissional de design para ilustrar o Folheto Digital partindo das ideias contidas no corpo da dissertação e consulta pessoal a adolescente Isabela Silva Ribeiro
Digital	Ao final, o Folheto será disponibilizado de maneira virtual e em alta resolução

Fonte: Elaborado pelo Autor (2020).

Com relação à escolha do público alvo aconteceu em virtude da ampla abrangência legislativa do ECA sendo que há inúmeros direitos desses interessados que necessitam de tutela diante da problemática do *Ciberbullying,* como os direitos ao respeito, a dignidade da pessoa humana, intimidade, privacidade, imagem, liberdade de expressão, crença, pensamento, segurança, proibição de tratamento desumano e cruel, cultura, lazer e a saúde, inclusive neste caso as de ordem mental, física e psicossomáticas.

Neste caso houve a consulta pessoal da adolescente Isabela Silva Riberio, de 15 anos de idade (minha sobrinha), a respeito do conteúdo, clareza, coesão, precisão e entendimento da proposta contida no folheto e o *feedback* na verdade ocorreu conforme o esperado, ou seja, o escopo foi atingido em relação a mensagem contida no produto.

O produto aqui definido se amolda em uma problemática moderna e atual da sociedade mundial, pois as vítimas em sua plenitude são atingidas em sua honra, dignidade da pessoa humana, liberdade de expressão, de crença, suportam a violência física, moral e psicológica, são desrespeitadas, no tocante, a segurança, intimidade, imagem, privacidade, ou seja, em qualquer ambiente, portanto, esses bens jurídicos estão devidamente tutelados pela Constituição Federal de 1988 e por disposições legais vigentes no Brasil, incluindo a proibição de tratamento desumano e cruel.

Essas intolerâncias desses indivíduos agressores tornam para a potencial vítima do *bullie virtual,* simplesmente impossível de conviver de maneira favorável e harmoniosa, aí dessa maneira haverá o atingimento da saúde psíquica do vulnerável, trazendo ainda consequências como a plena ausência de paz de espírito, a tranquilidade espiritual e outros. Por fim, o folheto a ser elaborado conterá dicas e assuntos relativos à prevenção do *Ciberbullying* como contribuição da academia em prol dos jovens da sociedade brasileira.

O Folheto Digital foi elaborado pelo Autor e ilustrado pelo desenhista e designer Matheus Lima Furtado, da cidade de Santa Cruz do Sul, no Estado do Rio Grande do Sul.

Figura 7 – Produto de Mestrado Profissional

Fonte: Elaborado pelo Autor e Ilustrado por Matheus Furtado (2020)

Quadro 3 - Proposta de Elaboração do Produto Profissional da Dissertação

Quadros	Frases elaboradas	Referências
1	Não é brincadeira, mas uma demonstração de poder, portanto, uma intimidação sistemática *on line*	Elaborado pelo Autor após leituras dos materiais relacionados na bibliografia deste trabalho como: - Cartilhas; - UNICEF; - UNESCO; - *SAFERNET* e Lei nº 13.185/2015
2	São ações verbais, morais, sexuais, sociais, psicológicas e virtuais, todas intencionais e repetitivas, que discriminam, aliados a comentários pejorativos, desenhos depreciativos, expressões preconceituosas graves, pois possuem o claro objetivo de agressão causando dor e angústia a vítima	Artigos 2º e 3º, ambos da Lei nº 13.185/2015, que institui o Programa de Combate à Intimidação Sistemática (***Bullying***)
3	Alguns se divertem, enquanto outros são mal tratados e humilhados, chantageados e ofendidos.	Elaborado pelo Autor após leituras de materiais relacionados na bibliografia deste trabalho como: - Cartilhas; - UNICEF; - UNESCO; - *SAFERNET* e Lei nº 13.185/2015
4	A exposição em ambiente digital é constante	Elaborado pelo Autor após leituras dos materiais relacionados na bibliografia deste trabalho como: - Cartilhas; - UNICEF; - UNESCO; - *SAFERNET* e Lei nº 13.185/2015
5	Atos de humilhação, insulto, intimidação, ameaças, preconceito e apelidos pejorativos	Elaborado pelo Autor após leituras dos materiais relacionados na bibliografia deste trabalho como: - Cartilhas; - UNICEF; - UNESCO; - *SAFERNET* e Lei nº 13.185/2015
6	Provocam constrangimentos psicológicos e psicossocial	Elaborado pelo Autor após leituras dos materiais relacionados na bibliografia deste trabalho como: - Cartilhas; - UNICEF; - UNESCO; - *SAFERNET* e Lei nº 13.185/2015

Fonte: Elaborado pelo Autor (2020)

A finalidade do folheto digital possui respaldo legal nos artigos 1º e 2º, da Lei nº 13.185/2015, pois menciona o combate a intimidação sistemática (*bullying*), que

trata de toda a conduta de violência física ou psicológica de maneira intencional e repetitiva e o objetivo gira em torno do fornecimento de conhecimento ao público vulnerável, por meio do uso das plataformas digitais muito presentes na vida desses jovens.

O produto tem o escopo de fornecer conhecimento ao público jovem, diante da prática da conduta de *Ciberbullying,* sendo que a ideia da divulgação pela crescente popularidade do marketing digital seria por meio das redes sociais, *Facebook*, *Telegram*, *Instagram*, *Whatsapp* e outras, muito presente no cotidiano desses indivíduos.

A aplicação do produto será por meio da divulgação nas redes sociais, que na verdade são os locais onde essa categoria de público se encontra com mais frequência, bem como em uma escola polo do Grande ABC, situada na cidade de Santo André/SP.

5 CONSIDERAÇÕES FINAIS

Este trabalho desenvolveu a interessante temática da Cidadania Digital na Prevenção da conduta de *Ciberbullying,* com o escopo direcionado a um público alvo de adolescentes e jovens na faixa etária de 12 a 18 anos de idade, sendo esse grupo considerado vulnerável pela legislação vigente brasileira e internacional, pois está tutelado em seus direitos fundamentais, abrangidos tanto pelo Estatuto da Criança e Adolescente (ECA), Lei de Combate a Intimidação Sistemática, LGPD, MCI, como pelo artigo 227, da Constituição Federal de 1988 e em âmbito internacional como tratados e convenções que o Brasil participa.

O estudo abarcou desde aspectos de cidadania, como de educação digital, segundo menciona a Lei nº 12.965 conhecida como Marco Civil da *Internet*, em seu artigo 26, entende que o cumprimento é dever constitucional do Estado Brasileiro na prestação dos serviços de educação, em todos os níveis de ensino inclusive.

Nesse rol se inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da *internet*, como ferramenta de exercício da cidadania, da promoção da cultura e do desenvolvimento tecnológico, assim se verifica o respaldo legal para a implementação dos institutos da Cidadania e Educação Digital, na identificação e prevenção do *Ciberbullying*.

Esse precioso pilar educacional virtual é entendido como o conjunto de metodologias que refletem ensino e aprendizagem, com o notório objetivo de transmitir conhecimentos éticos, morais e de cidadania digital as pessoas, para o uso e acesso em plataformas tecnológicas digitais, *internet*, aplicativos, programas e demais sistemas informatizados, respeitando sempre a dignidade da pessoa humana e o bem comum, que consequentemente caminhará para o interesse público naturalmente.

Com relação à privacidade de dados pessoais é medida de extrema necessidade hoje diante do crescimento exponencial das tecnologias digitais (TIC) colocadas à disposição desse público jovem, que na verdade são consideradas pessoas vulneráveis segundo as normas jurídicas em vigor, como é o caso ora estudado nesta dissertação, ou seja, crianças e adolescentes, portanto, os estabelecimentos comerciais, as empresas, escolas e demais organizações deverão atualizar seus procedimentos internos, suas políticas de utilização, bem como seus

termos de uso, a fim de se adequarem à legislação em vigor (LGPD) e não apenas em ato temerário a possíveis sanções legais que porventura possam suportar, mas visando sempre o melhor bem estar do menor envolvido, conforme as tutelas vigentes de proteção legais.

Claro que a segurança desse jovem público deve ter uma atenção mais do que especial pelas autoridades competentes, inclusive das que legislam neste país, pois o que se busca na realidade é o melhor interesse combinado com o bem-estar desse grupo, no que pese serem indivíduos íntimos das TIC, ainda desconhecem a verdadeira capacidade de compreensão em relação aos seus dados pessoais disponibilizados a terceiros.

Ainda essas informações representam a privacidade do menor, outrossim, com um significativo valor monetário, logo a LGPD surgiu como uma excelente contribuição legislativa perante o entendimento da proteção integral desses indivíduos alvo dessa pesquisa. Ainda é relevante trazer como oportuno e conveniente que a data de *07 de abril é considerado o Dia Nacional de Combate à violência na escola conhecida como bullying,* demonstrando assim a magnitude da problemática.

A *Safernet* é uma ONG (Organização Não Governamental) no Brasil, que promove a defesa desses direitos humanos na rede de *internet,* atuando na orientação e educação de crianças, adolescentes e jovens, bem como de pais e educadores sobre o uso responsável e seguro da *internet.* Juntamente com a UNICEF, ambas encabeçaram uma campanha de conscientização pelo combate à violência conhecida como *bullying.*

A UNICEF é a única organização mundial que se dedica especificamente às crianças, é uma agência oriunda das Nações Unidas, enquanto a UNICEF é regida pelos direitos da criança e trabalha para que essas conquistas (direitos) se convirjam diretamente em princípios éticos, morais permanentes e em códigos de conduta internacionais com o forte escopo nas crianças, a sigla significa Fundo das Nações Unidas para a Infância.

Com relação ao *Ciberbullying,* que se trata de uma temática moderna inserida na sociedade, a pessoa tem a sua honra, a dignidade humana, liberdade de expressão, intimidade, imagem e privacidade, simplesmente desrespeitados e com isso se torna praticamente impossível a convivência harmônica, com outros indivíduos na coletividade.

Os danos que a vítima suporta são variados e se estendem desde o aspecto psicológico do indivíduo, até sinais de baixa autoestima, com desenvolvimento inclusive de problemas patológicos, esse público vítima do *Ciberbullying* manifesta temor de se expressar publicamente, possuem fobia social, quadros depressivos, evitam o contato com pessoas e principalmente necessitam da atenção de profissionais experientes e especialistas.

Assim entendo que os pilares, Cidadania e Educação Digital se mostram eficientes, sendo uma atitude indispensável para uma boa compreensão e fomento do uso responsável da *internet,* pois possui obediência a aspectos éticos, morais, do uso responsável dos recursos tecnológicos disponibilizados e do usufruto consciente de todos esses benefícios, por isso, dá pertinência e relevância para esses institutos mencionados.

A Educação Digital que encontra seu respaldo legal no artigo 26, do MCI, diante de um público alvo vulnerável que são os jovens adolescentes e tutelados por diversas legislações vigentes no Brasil e inclusive no exterior. Ainda temos a LGPD, que sugere uma interpretação legislativa favorável a esse público vulnerável, segundo entendimento do próprio ECA e da Constituição Federal de 1988.

O *Ciberbullying* é uma prática ilegal, irregular, ofensiva, injusta e cruel que atingiu um nível de inquietação, incômodo e afligimento tamanho no mundo moderno, pois tal prática assola as vítimas em seu estado mental, por meio de quadros patológicos delicados, pouca ou nenhuma estima pessoal, imenso temor social dentre outros quadros depressivos, que trazem a plena infelicidade, baixa produtividade escolar e o efetivo transtorno de espírito.

A LGPD também contribui para uma realidade melhor para esses interessados, pois o bem-estar dos indivíduos desse grupo e o seu melhor interesse devem ser interpretados de uma maneira mais favorável, no tocante, a proteção de dados e da privacidade do menor impúbere.

O peso da transformação digital pode ser analisado diante de uma grande engrenagem, pois os indivíduos, empresas, governos e órgão públicos possuem um papel fundamental nesse contexto de modernidade, as TIC hoje são realidade e necessárias para o relacionamento de pessoas, para requerimentos de serviços públicos com mais eficiência e também a satisfação de clientes de empresas privadas, assim o retrocesso já não mais possível diante da atual conjuntura.

Ainda é possível entender que há campo para estudos futuros, acerca desta temática relevante e preocupante socialmente, pois envolve o bem-estar combinado com o melhor interesse desse público, que estão em consonância com os princípios da universalização e responsabilidade pública, trazidos pela Constituição Federal de 1988.

A vitimização desse grupo diante da prática de atos criminosos influi na saúde mental e consequentemente acarretará doenças oriundas da mente, que se manifestam, como pensamentos, percepções, emoções variadas, comportamentos diversos, como também a depressão e a ansiedade.

Em questões de aprendizado é salutar dizer que foi proveitoso à dedicação a este trabalho, pois assim houve a possibilidade de entender o quão é grave a conduta delitiva do *Ciberbullying* na vida do jovem e ainda como são necessários os conceitos de Cidadania e Educação Digital nos dias atuais.

REFERÊNCIAS

ABRACE. ***Cyberbullying*** **pode aumentar durante a pandemia de covid-19, diz especialista.** Curitiba, 5 de maio de 2020. Disponível em: https://abraceprogramaspreventivos.com.br/cyberbullying-pode-aumentar-durante-a-pandemia-de-covid-19/ Acesso em 03 de agosto de 2020.

ABRUSIO, Juliana (Coord.). **Educação Digital**. 1. ed. São Paulo: Revista dos Tribunais, 2015.

ALMEIDA, Maria Paula Castro de. **A evolução no combate aos crimes virtuais.** Escola da Magistratura do Rio de Janeiro, 2015. Disponível em: https://www.emerj.tjrj.jus.br/paginas/trabalhos_conclusao/1semestre2015/pdf/MariaPaulaCastrodeAlmeida.pdf. Acesso em 06 jun. 2020.

BARRETO, Alessandro Gonçalves; ARAÚJO, Vanessa Lee. **Vingança Digital** – Compartilhamento não Autorizado de Conteúdo Íntimo na *Internet*, Procedimentos de Exclusão e Investigação Policial. 1.ª ed, Rio de Janeiro/RJ: Editora Mallet, 2017.

BASTOS, Angélica Barroso, ARAÚJO, Camila Felix, ALMEIDA, Eduarda Lorena de, AIEXE, Egídia Maria de Almeida e GOMES, Marcella Furtado de Magalhães. **Direitos Humanos e Cidadania** - Proteção, Promoção e Restauração dos Direitos das Crianças e Adolescentes.V.15. Belo Horizonte: Marginália Comunicação, 2016.

BONFIM, Natália Bertolo. **MP 869/18 e alterações na LGPD**. Migalhas. São Paulo: 03 de janeiro de 2019. Disponível em: https://www.migalhas.com.br/dePeso/16,MI293658,71043-MP+86918+e+alteracoes+na+LGPD Acesso em: 14 mai. 2019.

BRASIL, CERT. Cartilha de Segurança Para *Internet*, versão 4.0/CERT. br–São Paulo: Comitê Gestor da *Internet* no Brasil. 2012.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União.** Poder Legislativo. Brasília, DF, 05 out. 88. Seção 1, p. 1.

BRASIL. Lei nº 13.718 de 24 de setembro de 2018 que dispõe sobre os crimes de importunação sexual e de divulgação de cena de estupro. **Diário Oficial da União**, Poder Legislativo. Brasília, DF, 25 set. 2018. Seção 1, nº 185, p. 2.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais. **Diário Oficial da União**, Poder Legislativo. Brasília, DF, 15 ago. 2018. Seção 1, nº 157, p. 59.

BRASIL. Lei nº 13.663 de 14 de maio de 2018 que dispõe sobre a inclusão e promoção de medidas de conscientização, de prevenção e de combate a todos os tipos de violência e a promoção da cultura da paz nos estabelecimentos de ensino. **Diário Oficial da União**, Poder Legislativo. Brasília, DF, 15 mai. 2018. Seção 1, nº 92, p. 1.

BRASIL. Lei nº 13.185 de 06 de novembro de 2015 que dispõe sobre a Instituição do Programa de Combate à Intimidação Sistemática (*Bullying*). **Diário Oficial da União**, Poder Legislativo. Brasília, DF, 09 nov. 2015. Seção 1, nº 213, p. 1.

BRASIL. Lei nº 12.965 de 23 de abril de 2014 que estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. **Diário Oficial da União.** Poder Legislativo. Brasília, DF. 24 abr. 14. Seção 1, p. 1.

BRASIL. Ministério Público Federal (MPF). Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.

BRUNO, Fernanda. Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade. **Porto Alegre: Sulina**, p. 123, 2013.

BRUNO, Fernanda. Rastrear, classificar, performar. **Ciência e Cultura**, v. 68, n. 1, p. 34–38, 2016. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252016000100012>. Acesso em: 5 Dez. 2020.

CARNEIRO, Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação.** Âmbito Jurídico. 01 de abr. de 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/. Acesso em: 09 de jun. 2020.

CASTELLS, Manuel. **O poder da comunicação**. Fundação Calouste Gulbenkian, 2013.

CONSULTOR JURÍDICO. **Maior celeridade:** CCJ do Senado aprova criação dos juizados especiais criminais digitais. 12 dez. 18. Disponível em: https://www.conjur.com.br/2018-dez-12/ccj-senado-aprova-criacao-juizados-especiais-criminais-digitais - Acesso em: 25 mai. 2019.

CORDEIRO, Salete FN; BONILLA, Maria HS. **Educação e tecnologias digitais: políticas públicas em debate.** Passo Fundo, RS: SENID, 2018.

DAMASIO DE JESUS apud ARAS, Vladmir. **Crimes de informática:** Uma nova criminalidade. Disponível em: https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em 25 mai. 2020.

DA SILVA JUNIOR, Sady Darcy; LUCIANO, Edimara Mezzomo; LÜBECK, Rafael Mendes. Revalidação da escala mobile users' information privacy concerns para o contexto brasileiro. **Revista Eletrônica de Ciência Administrativa**, v. 19, n. 2, p. 280-298, 2020.

DESLANDES, Suely Ferreira; COUTINHO, Tiago. O uso intensivo da *internet* por crianças e adolescentes no contexto da COVID-19 e os riscos para violências autoinflingidas. **Ciência & Saúde Coletiva**, v. 25, p. 2479-2486, 2020.

DI FELICE, M.; PIREDDU, M.; DE KERCKHOVE, D.; BRAGANÇA DE MIRANDA, J.; SANCHEZ MARTINEZ, J. A.; ACCOTO, C. Manifesto pela Cidadania Digital. **Lumina**, v. 12, n. 3, p. 3-7, 30 dez. 2018.

DUARTE, Jorge. Comunicação pública. **São Paulo: Atlas**, p. 47-58, 2007.

EPM. Escola Paulista da Magistratura. **Direito Digital e Proteção de Dados Pessoais**, Cadernos Jurídicos, Ano 21, nº 53, Janeiro-Março de 2020, ISSN 1806-5449, São Paulo, p.1-202

FIDALGO, Augusto. **Educação Digital. Aspectos conceituais.** Administradores.com. 17/04/2019. Disponível em: https://administradores.com.br/artigos/educacao-digital-aspectos-conceituais - Acesso em 25 mai. 2019.

FIESP. Cartilha FIESP/CIESP – **LGPD - Lei Geral de Proteção de Dados** – São Paulo: FIESP, 2018. 24 p.

GEEKIE. **Educação Digital: o passo necessário na formação da cidadania (digital).** 17 jan. 18. Disponível em: https://www.geekie.com.br/blog/educacao-digital-2/ Acesso em 02 jun. 2019.

GIL, Antônio Carlos. **Métodos e Técnicas de Pesquisa Social**. 7. ed. São Paulo: Atlas, 2019.

JENKINS, Henry. **Cultura da convergência**. Aleph, 2015.

JORGE, Higor Vinicius Nogueira. **Solução para o *cyberbulling* não é restrita à escola.** Consultor Jurídico. 08 de jun. 2011. Disponível em: https://www.conjur.com.br/2011-jun-08/solucao-cyberbullying-nao-responsabilidade-escola-policia. Acesso em: 02 jun 2020.

JORNAL GLOBO. **Vazamento de dados dos hotéis Marriott pode ter afetado 500 milhões de clientes**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2018/11/30/vazamento-de-dados-dos-hoteis-marriott-pode-ter-afetado-500-milhoes-de-clientes-diz-a-rede.ghtml - Acesso em 07 mar. 2019.

KIGERL, Alex. Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. **International Journal of Cyber Criminology**, v. 10, n. 2, 2016.

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

MARTINS FILHO, Ives Gandra da Silva. O princípio ético do bem comum e a concepção jurídica do interesse público. **O princípio ético do bem comum e a concepção jurídica do interesse público**, 2000.

MIGALHAS. **Proteção de dados pessoais deverá entrar na Constituição como direito fundamental.** Disponível em:

https://www.migalhas.com.br/Quentes/17,MI305569,101048-Protecao de dados pessoais deverá entrar na Constituição como direito. Acesso em 26 de julho 2019.

MILAN, Matthew; MASS, Critical. ***Backcasting* 101.** 10 de abril de 2008. USA. Disponível em: https://www.slideshare.net/mmilan/backcasting-101-final-public. Acesso em: 20 set. 2019.

MPSP - MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. ***Bullying* Não é Legal.** 2010. Disponível em: http://crianca.mppr.mp.br/pagina-1756.html. Acesso em: 02 de agosto de 2020.

MPSP - MINISTÉRIO PÚBLICO DO ESTADO DE SÃO PAULO. **Tolerância.** 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/Cartilhas/Tolerancia_cartilha_Impressao.pdf. Acesso em: 02 de agosto de 2020.

MINUTO DA SEGURANÇA. **Israel neutraliza o Ataque Cibernético explodindo um edifício com hackers.** Disponível em: https://minutodaseguranca.blog.br/israel-neutraliza-o-ataque-cibernetico-explodindo-um-edificio-com-hackers/. Acesso em 01 jun. 2019.

MIRONOVA, Olga A.; BOGDANOVA, RM; KOLESNIKOV, Yuri A. Aspectos da aplicação da Teoria Generacional no desenvolvimento da Educação Digital na Rússia. **Медиаобразование**, n. 1 de 2019.

MISTURA, Rebecca. *Cyberbullying* acontece 70% nas redes sociais. Diário da Manhã. 04 ago. 2018. Disponível em: https://diariodamanha.com/noticias/cyberbullying-acontece-70-nas-redes-sociais/ - Acesso em: 08 jun. 2020.

NAKAGAWA, Liliane. **Previdência privada do Banco do Brasil vaza dados de 153 mil clientes.** Olhar Digital. 06 de mai. 2020. Disponível em: (https://olhardigital.com.br/noticia/-exclusivo-banco-do-brasil-vaza-dados-pessoais-de-153-mil-clientes/100395). Acesso em: 15 mai. 2020.

NORTON. **Relatório de crimes cibernéticos Norton:** O impacto humano. Symantec Company. EUA, Mountain View: 2018. 32p.

OLHAR DIGITAL. **Israel é o primeiro país a responder a um ciberataque com força militar.** São Paulo: 06 mai. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/israel-e-o-primeiro-pais-a-responder-um-ciberataque-com-forca-militar/85477. Acesso em: 14 mai. 2019.

ORRIGO, Gabriel Marcos Archanjo; FILGUEIRA, Matheus Henrique Balego. **Crimes Cibernéticos**: uma abordagem jurídica sobre crimes realizados no âmbito virtual. Jus Brasil. Outubro de 2015. Disponível em: https://jus.com.br/artigos/43581/crimes-ciberneticos-uma-abordagem-juridica-sobre-os-crimes-realizados-no-ambito-virtual. Acesso em: 04 jun. 2020.

PIMENTEL, Jose Eduardo de Souza. Introdução ao Direito Digital. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, v. 13, n. 1, 2018.

PINHEIRO, Mirelle. **DF corre risco de se tornar paraíso de cibercriminosos internacionais.** Metropoles. Brasília: 12 de maio de 2019. Disponível em: https://www.metropoles.com/distrito-federal/df-corre-risco-de-se-tornar-paraiso-de-cibercriminosos-internacionais. Acesso em: 14 mai. 2019.

ROBINSON, J., BURCH, S., TALWAR, S., O'SHEA, M., WALSH, M. Envisioning sustainability: **Recent progress in the use of participatory *backcasting* approaches for sustainability research**, Technological Forecasting and Social Change, 2011, 78: 756-768.

RODRIGUES Fernando. Massacre em Christchurch, na Nova Zelândia: entenda o que se sabe até agora. **Poder 360**. 18 mar. 2019. Disponível em: https://www.poder360.com.br/internacional/massacre-em-christchurch-na-nova-zelandia-entenda-o-que-se-sabe-ate-agora/. Acesso em: 25 mai. 19.

RUTHERFORD, Mikhail. **Crimes na *internet*: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto.** Jusbrasil, 2015. Disponível em: https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-*internet*-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto. Acesso em 26 mai. 2019.

SAFERNET. **Campanha de Combate ao *Bullying***. 07 de abr. 2020. Disponível em: https://new.safernet.org.br/content/conheca-campanha-acabar-com-o-bullying-edaminhaconta - Acesso em: 23/04/2020.

SANTIAGO, Christopher. O que é cidadania digital? Aprenda tudo neste post. **SolutiResponde.** São Paulo, 21 de jan. de 2019. Disponível em: https://solutiresponde.com.br/o-que-e-cidadania-digital-aprenda-tudo-neste-post/. Acesso em 11 mai. 2020.

SILVA, Victor Hugo. **SUS é alvo de vazamento com dados de 2,4 milhões de usuários.** https://tecnoblog.net/285672/sus-vazamento-dados-usuarios/ - SUS – Acesso em 08 mar. 2019.

SIMULARE JOGOS VIRTUAIS. **Educação digital: saiba o que é e qual a sua importância.** 23 mai. 19. Disponível em: https://simulare.com.br/blog/educacao-digital-saiba-o-que-e-e-qual-a-sua-importancia/. Acesso em: 31 mai. 2019.

SOMADOSSI, Henrique. **O que muda com a Lei Geral de Proteção de Dados (LGPD).** 24 de agosto de 2018. MIGALHAS. Brasil: São Paulo, 2018. Disponível em:https://www.migalhas.com.br/dePeso/16,MI286235,31047-%20O+que+muda+com+a+Lei+Geral+de+Protecao+de+Dados+LGPD). Acesso em 27 mai. 2019.

SOUZA, Maurício de. A turma da Mônica em: O Estatuto da Criança e do Adolescente. São Paulo: Editora Maurício de Souza, 2006. Disponível em: https://irp-

cdn.multiscreensite.com/c70477cd//files/uploaded/equinha.pdf. Acesso em: de agosto de 2020.

STICKDORN, Marc; SCHNEIDER, Jakob. **Isto é *design thinking* de serviços: Fundamentos, ferramentas, casos**. Bookman Editora, 2014.

STRATTON L, POWELL A e R Cameron. **Crime e Justiça na Sociedade Digital: Rumo a uma 'Digital Criminologia'?** Jornal Internacional de Crime, Justiça e Democracia social 6 (2): 17-33, 2017. DOI: 10,5204 / ijcjsd.v6i2.355.

TAYLOR, Charles. A esfera pública. **Trad. Artur Mourão. Covilhã: Lusosofia Press**, 2010.

TSCHIMMEL, Katja. **Design Thinking como um kit de ferramentas eficaz para a inovação,** Anais da XXIII Conferência ISPIM: ação para a Inovação: Inovando pela Experiència . Barcelona, 2012. ISBN 978-952-265-243-0.

TONDO, Rômulo Oliveira. **Literacias e Juventudes: competências socioculturais para o século XXI.** Santa Maria/RS, 2016. Disponível em: https://www.ufsm.br/cursos/pos-graduacao/santa-maria/ppgd/wp-content/uploads/sites/563/2019/09/11.4.pdf. Acesso em 11 de jun. 2020.

TOALDO, Mariângela Machado; MARQUES, Jane A.; LIMA, Gustavo Fussieger de. **Literacia Digital: educação para a leitura de conteúdos midiáticos**. Em: IV CONEDU, v. 1, p. 1-12, 2017.

UNESCO, Organização das Nações Unidas para a Educação, a Ciência e a Cultura, Alfabetização Midiática e informacional, **Diretrizes para a formulação de Políticas e Estratégias**, 2016.

UNICEF. **Convenção sobre os Direitos da Criança.** 1990. Disponível em: https://uni.cf/38rvTJn. Acesso em: 21 jan. 2020.

USO INTENSIVO DAE PLATAFORMAS DIGITAIS DURANTE A PANDEMIA DO CORONAVÍRUS PODE EXPOR CRIANÇAS E ADOLESCENTES. **Jornal Cruzeiro**, Sorocaba, 15 de abril de 2020. Seção: Tecnologia. Disponível em: https://www.jornalcruzeiro.com.br/tecnologia/uso-intensivo-de-plataformas-digitais-durante-a-pandemia-do-coronavirus-pode-expor-criancas-e-adolescentes/. Acesso em 06 de agosto de 2020.

WEULEN KRANENBARG, Marleen; HOLT, Thomas J.; VAN GELDER, Jean-Louis. Offending and victimization in the digital age: Comparing correlates of cybercrime and traditional offending-only, victimization-only and the victimization-offending overlap. **Deviant Behavior**, v. 40, n. 1, p. 40-55, 2019.

WILSON, Chauncey. **Method 16 of 100: *Backcasting***. 02 de agosto de 2011. Disponível em: https://dux.typepad.com/dux/2011/08/method-16-of-100-backcasting.html. Acesso em: 19 set. 2019.