Educação Digital no enfrentamento do *Ciberbullying* e a Lei Geral de Proteção de Dados

Digital Education in the fight against Cyberbullying and the General Data Protection Law

Regina Rossetti
Doutora em Filosofia pela USP com pós-doutorado e Professora do Programa de Pós-Graduação em Comunicação pela Universidade de São Caetano do Sul - USCS. Email: regina.rossetti@online.uscs.edu.br

Ciro Ferreira da Silva Junior
Mestre pelo Programa de Pós-Graduação em Inovação na Comunicação em Interesse Público (PPGCOM), da Universidade Municipal de São Caetano do Sul (USCS). Bacharel Graduado em Ciências Jurídicas pela Faculdade de Direito de São Bernardo do Campo (2007). Email: ciro.junior@uscsonline.com.br

Resumo
A Cidadania Digital no enfrentamento 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. É 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 O estudo compreende um delineamento, por meio de uma abordagem qualitativa do tipo exploratória, revisão bibliográfica e documental. Assim foi elaborado um Folheto Digital que traz subsídios para a compreensão dessa problemática moderna que denota entendimento de fato do saber, conhecer e mensurar os riscos do uso frequente da rede de internet pelo público jovem, situado principalmente na faixa de 12 a 18 anos de idade, além de saber que de virtual não há absolutamente nada, pois esses ambientes funcionam em tempos reais combinando e integrando elementos, informações, dados e visualizações. Os resultados mostram que 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, 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 do folheto, com o escopo de identificar e prevenir a conduta do Ciberbullying.

Palavras-Chave
Educação Digital; Cidadania Digital; Ciberbullying; Proteção e Privacidade de Dados.

Abstract
Digital Citizenship in the fight against 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. It is a problem present in contemporary world society, especially during the Covid-19 pandemic period, which occurred in 2020, as the victim has his honor, human dignity, freedom of expression, intimacy, image, privacy and other affronts, legal assets valuable that are duly protected by constitutional provisions in force in Brazil The study comprises an outline, through a qualitative approach of the exploratory type, bibliographic and documentary review. In this way, a Digital Brochure was created that provides

subsidies for understanding this modern issue that denotes a de facto understanding of knowledge, knowing and measuring the risks of frequent use of the internet network by young audiences, located mainly in the 12 to 18 year old age group. in addition to knowing that there is absolutely nothing virtual, as these environments work in real time combining and integrating elements, information, data and visualizations. The results show that 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, which brings protection, transparency and regulation about personal data citizens in the country, covering 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 preparation of the brochure, with the scope of identifying and preventing the conduct of Cyberbullying.

Keywords
Digital Education; Digital Citizenship; Cyberbullying; Data Protection and Privacy.

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, Signal, 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, estudos e pesquisas 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 no 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 fator essencial de 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 hoje após a pandemia do Covid-19, 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 no ambiente escolar, seja em estabelecimento público ou privado, invocando para isso, se necessitar até os aspectos da interdisciplinaridade disponibilizados no 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 inserida em uma sociedade da informação, pois o regresso tecnológico é impossível e impraticável, 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 à 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 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 no contexto da aprendizagem seja escolar, de trabalho, mesmo de lazer, enfim, representa a efetividade da integração das pessoas ao mundo e desse mundo moderno com 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. 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.

Cidadania Digital

A conectividade é parte integrante das variadas rotinas do dia a dia dos indivíduos, levando em conta os aspectos da efetiva existência da rede de *internet*, contudo, há a necessidade da utilização da rede 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 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 de direitos e deveres, que na verdade são originados segundo a Constituição Federal de cada país, ou mesmo de uso e costumes, versam a respeito de um mundo virtual, assume 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 (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, 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 cibernéticoscomo *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 princípios, valores, ações e 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 e deveres, e os direitos são necessários. Os *softwares*, regras, algoritmos devem estar estruturados em garantia aos direitos dos indivíduos e não o contrário (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 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 inseridas em ambientes digitais (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 efetiva 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.

Ciberbullying

As Tecnologias da Informação e da Comunicação se mostram cada vez mais presentes no dia a dia das empresas, dos cidadãos em geral, do poder público e 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, estatal e dos cidadãos, mas sim de indivíduos mal-intencionados e maliciosos, que utilizam as TIC, para uma finalidade nada ética e sim criminosa como os conhecidos delitos de estelionato, furto mediante fraude, pornografia de menores de idade, *Ciberbullying* dentre outros.

O *bullying* é uma ação ofensiva, injusta, irregular e bárbara, que abarca 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.

O fato é que no caso dos jovens que representarão em um futuro muito próximo para a nossa sociedade, pessoas com uma notável baixa autoestima aliada a outros sintomas gerados pela prática ofensiva do *Ciberbullying*, trarão malefícios a saúde desse público envolvido.

A vítima do *Ciberbullying*tem sua honra, dignidade humana, liberdade de expressão, intimidade, imagem e privacidade, ou seja, todos estes bens jurídicos que são devidamente protegidos pela legislação brasileira atingidos, sendo que as intolerâncias dos 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 que é considerada Dia Nacional de Combate ao *bullying*, a*Safernet* e a UNICEF lançaram uma campanha de conscientização pelo combate ao *bullying* (SAFERNET, 2020).

A Lei nº 13.663/18 em seu artigo 12, inciso IXinstitui 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.

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, mas também está destoando outras escaladas criminosas que antes não se falavam a respeito, dentre elas os 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 e temor 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 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 do 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 aos olhos do homem médio, portanto, a conduta do autor destrói a boa reputação da pessoa atingida (vítima), como também causa enormes estragos 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, denegrindo sua imagem pessoal perante a sociedade em geral, ao ambiente de trabalho e escolar (BARRETO; ARAÚJO, 2017).

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

A *divulgação/exposição* de materiais íntimos não autorizados em que participam crianças e adolescentes são considerados atos criminosos, 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 pela 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 desenvolvidas no ambiente digital 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 e por meio de uma relação interpessoal assimétrica, evidenciada por explícita dominação (BASTOS *et al.*, 2016).

Os resultados dessas condutas realizadas em ambiente virtual 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 (MISTURA, 2018).

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

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

A doença conhecida atualmente 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, pesquisas, tarefas, lazer, como também em contatos sociais entre amigos, familiares e para outros fins desejados (DESLANDES; COUTINHO, 2020).

Contudo, houve um aumento significativo das interações entre pessoas no contexto do ambiente digital, fazendo a sociabilidade digital avançar demasiadamente, gerando outro efeito concreto que foi a hiperexposição que abrange uma diminuição das fronteiras entre o aspecto público e privado dos 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 de *Ciberbullying* (ABRACE, 2020).

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

Os educadores, muitas vezes trabalhando de suas casas, 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 feroz 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 incial de confinamento social da pandemia da Covid-19, foi registrada uma alta de 25% no número de conexões de download referente a material impróprio na Espanha e em outros países do continente europeu (USO..., 2020).

Nesse momento, os pais desempenham um papel de extrema valia, pois podem exercer uma supervisão de acessos às 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).

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 atualmente 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*.

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

Os delitos descritos na Lei nº 13.718/18, de 24 de setembro de 2018 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.

A pornografia de vingança é uma modalidade que envolve um conteúdo de cunho sexual, portanto, íntimo e que 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, humilhações, embaraços e até ameaças, causando um profundo incômodo.

Claro que tais divulgações são impróprias, inoportunas, injustas, cruéis e ofensivas, mas na verdade, são literalmente consideradas 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, psíquica, 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 Brasileiro, 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.

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 públicos, instituições e empresas particulares ou públicas, de terem seus dados e informações transmitidos a terceiros de maneira restritiva, ou seja, somente nas hipóteses especificadas e individualizadas 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, é 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 desse usuário (DA SILVA JUNIOR *et al.*, 2020).

A Lei Geral de Proteção de Dados (LGPD) nº 13.709/18, se espelhou no Regulamento Geral de Proteção de Dados europeu (EPM, 2020 e 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 e transferência. (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 na literatura, como a privacidade na concepção de 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).

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.

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*.

Por fim, o desafio de manter a privacidade de dados e informações está lançado, pelo aumento significativo 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).

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, sejam esses familiares e/ou amigos, trouxe um amplo acesso as TIC, sem, contudo, levar em conta as distâncias territoriais. Ainda deverá ser observado, que de acordo com o entendimento da revista *The Economist,* "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 1.988, 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, portantotodos devem estar conscientes de suas responsabilidades de proteção (EPM, 2020).

Segundo o relatório da UNICEF (Fundo das Nações Unidas para a Infância) de 2018 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 pelas tratativas da 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 em vigor.

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 1.988, o ECA, a Convenção sobre os Direitos da Criança com status de Tratado Internacional de Proteção de Direitos Humanos (EPM, 2020).

A Constituição Federal (C.F.) 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 1.988 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 das 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 por meio do Decreto nº 99.710/1990 (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.

Na seara da tutela dos vulneráveis ocorre a fiel proteção, aliás em sua integralidade, sendo que essas 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).

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

Inicialmente os dados considera dado pessoal como informação relacionada à pessoa natural identificada e indentificável (BRASIL, 2018). O tratamento de dados se refere a operação e classifica em 20 verbos que nada mais são do que ações que disciplinam distintas maneiras de tratamentos de dados pessoais desses indivíduos.

Os provedores de *internet*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). No caso do estabelecimento escolar possuir os dados relativos a identificação de jovens (alunos), 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 e compreensão (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 (EPM, 2020).

Assim, a ausência de consentimento do interessado será consagrado como de caráter ilícito, ofensivo, irregular e injusto, bem como sujeito as sanções legais (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).

A responsabilidade sob a ótica da LGPD

O escopo da LGPD visa à 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 esteja localizada, 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 à arte, editoriais, 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, como também é relevante salientar que estabelecimentos comerciais como hotéis, faculdades, fábricas, colégios dentre outros (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 *conscientização* dos envolvidos na problemática de dados pessoais na utilização das TIC (EPM, 2020).

Um bom exemplo, para um entendimento útil em relação à aplicação da LGPD na prática, 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 (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 argumentar 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 (EPM, 2020).

A atuação escolar do aluno é outro fator importante de análise, pois há a possibilidade de torná-lo plenamente identificável, sob as 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).

Procedimentos Metodológicos

O estudo compreende 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 brasileira, 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 procedimentos quantitativos aplicados, contudo, a diferença de ambos versa acerca de termos numéricos obtidos, 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 como *Ciberbullying* e a Proteção e Privacidade de Dados, 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 dessa 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, 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.

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.

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.

Após a revisão da literatura e análise da legislação brasileira, foi proposta a elaboração de um folheto digital direcionado a crianças e adolescentes de 12 a 18 anos com a finalidade de prevenção da prática de Ciberbullying, conforme apresentado no Quadro 1.

Quadro 1 - Proposta de Elaboração do Folheto Digital

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 de um papel sulfite branco A4 em partes, excluindo o cabeçalho
Ideia de elaboração	Contratação de um profissional de design para ilustrar o Folheto Digital partindo das ideias obtidas a partir da literatura, análise da legislação brasileira e consulta pessoal a adolescente Isabela Silva Ribeiro
Digital	O folheto será disponibilizado de maneira virtual e em alta resolução nas redes sociais

Fonte: Elaborado pelos Autores (2020)

A consecução também abarcou os cenários nos quais os criminosos se inseriram para a consumação dessas práticas delituosas, 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.

Análise e Discussão dos Resultados

A tecnologia atual está indiscutivelmente presente no dia a dia das pessoas, 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, 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 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).

Pinheiro (2019) expôs uma realidade preocupante, 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 a fraude bancária, comercialização de dados via *deep* e *dark web*, ambas acessadas por meio do navegador conhecido como TOR.

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

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, onde ocorreu uma falha na segurança que afetou todo o

sistema de reservas do hotel (conhecido por *starwood)* e que pode ter prejudicado cerca de 500 milhões de pessoas, em virtude da ação de hackers que devastaram nomes, números de telefones, cartões de crédito, inclusive com as respectivas datas de vencimentos, e-mail, números de passaportes, datas de nascimentos e dados de chegadas e saídas 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, 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 a partir do número do cartão do serviço e uma senha (SILVA, 2019).

Em um site do BB Previdência houve 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 explícita 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 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 com o intuito de subsidiar medidas de identificação e correção para salvaguardar o perfeito sigilo de informações de clientes (NAKAGAWA, 2020).

Com relação ao termo *Ciberbullying* objeto desse artigo científico, por exemplo, utilizado repetidamente e intencionalmente com o intuito de proferir atos de violência contra outro ser humano, 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 infelizmente 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 constrangimento junto à rede mundial de computadores, que nesse caso são utilizados os meios próprios da *internet* para atacar o jovem com ações depreciativas, violentas, exibição de fotos alteradas, mas que possibilitam a identificação do menor vítima da prática cruel (BARRETO; ARAÚJO, 2017).

As condutas do envio de fotos e vídeos conhecidos por *nudes* são hábitos costumeiros entre o público jovem, 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 (BARRETO; ARAÚJO, 2017).

A sanção social em desfavor desse público jovem, infelizmente são enérgicas, severas e doloridas, que podem gerar até perseguições em estabelecimento escolar, em locais públicos e que muitas das vezes essas vítimas suicidam em virtude do imenso sofrimento que causaram em suas famílias. Contudo o indivíduo responsável por essa prática nociva tem a óbvia intenção de deteriorar a imagem, privacidade e intimidade, com o escopo de causar um profundo sofrimento e a infâmia pública ao jovem (BARRETO; ARAÚJO, 2017).

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, para a efetiva prevenção e combate aos tipos de violência existentes hoje (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 apresenta como princípios a liberdade de expressão, comunicação, manifestação de pensamento, assim como na Constituição Federal de 1.988 e a proteção da privacidade, dos dados pessoais, nos termos do artigo 3º, da lei. 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).

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

Pimentel (2018) entende também que embora o MCI tutele direitos de cunho civis na 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.

A Lei Geral de Proteção de Dados nº 13.709/18, conhecida popularmente como LGPD, traz sua aplicação a qualquer pessoa, seja natural ou jurídica 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 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 portes são obrigadas a tratar os dados pessoais, bem como atender os princípios da finalidade (propósitos legítimos) para o tratamento de dados, adequação (compatibilidade), necessidade (mínima coleta) e transparência (FIESP, 2018).

O dado pessoal está definido no artigo 5º, I, da LGPD como a informação relacionada a pessoa natural identificada ou identificável, dos 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. A LGPD também 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, nos termos do artigo 5º, X, se resume a toda operação realizada com dados pessoais, 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 como para quem trata dados pessoais que devem se na lei (FIESP, 2018).

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* desenvolvidas e difundidas, com um sério e comprometido planejamento prévio, aliado à eficácia na implementação e gestão dos recursos estatais (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 1.988 (BRASIL, 1988), porque o cidadão somente terá o conhecimento necessário e real sobre os aspectos de segurança da informação com uma orientação educacional digital elevada, pois os crimes cometidos em ambiente cibernético 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 e crimes contra a incolumidade das pessoas.

Aliado ao fato das legislações abordadas nessa temática tratarem da 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.

O instituto da Cidadania Digital na Prevenção dos *Ciberbullying* deverá ser compreendido como um dever de Estado, que por meio de políticas públicas eficientes que garantam o direito do indivíduo buscar informação e conhecimento junto a rede de internet para o exercício de 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*.

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, de forma a evitar a exposição exacerbada do indivíduo e as consequências indesejadas. As ausências dos institutos da Cidadania e Educação Digital proporcionam 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.

Como resultado da pesquisa foi elaborada 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*.

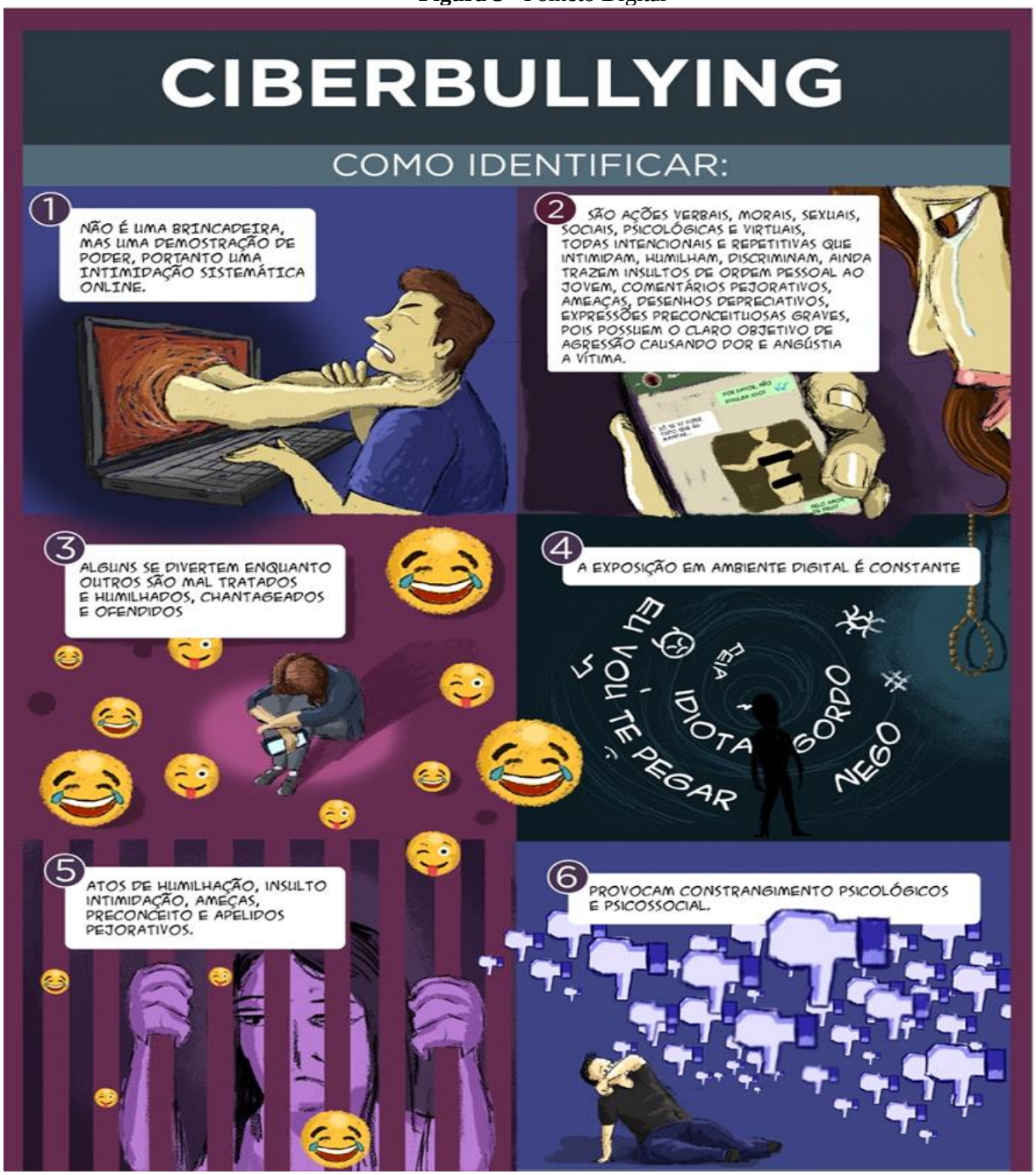
Quadro 2 - Proposta de Elaboração do Folheto Digital

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	
5	Atos de humilhação, insulto, intimidação, ameaças, preconceito e apelidos pejorativos	
6	Provocam constrangimentos psicológicos e psicossocial	

Fonte: Elaborado pelo Autor (2020)

O folheto digital é um material de comunicação de ordem prática, eficiente e com uma leitura rápida, que proporciona um entendimento sobre essa problemática tão presente de *Ciberbullying*, muito comum atualmente no mundo contemporâneo, conforme Figura 3.

Figura 3 - Folheto Digital



Fonte: Elaborado pelos Autores e Ilustrado por Matheus Furtado (2020).

Assim, o folheto digital 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.

A elaboração e divulgação do folheto digital por meios sociais contribui social e cientificamente para a divulgação de possíveis crimes cometidos pela *internet*, identificação das condutas que possam ser caracterizadas como criminosas e a existência de legislação brasileira protetiva, em especial às crianças e adoloscentes.

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, que é 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 1.988, tanto no 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, que entende que o cumprimento é dever constitucional do Estado Brasileiro na prestação dos serviços de educação, em todos os níveis de ensino.

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. Assim, 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 proteção é importante na medida em que 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, de 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 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.

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 . Educação Digital. **Revista dos Tribunais**, São Paulo: 2015.

BARRETO, Alessandro Gonçalves; ARAÚJO, Vanessa Lee. **Vingança Digital** – Compartilhamento não Autorizado de Conteúdo Íntimo na *Internet*, Procedimentos de Exclusão e Investigação Policial. Rio de Janeiro: 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.

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. **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.

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

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.

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, 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.

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

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

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.

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

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.

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.

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.

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.

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.

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.