

## A GLOBALIZAÇÃO E O TRATAMENTO JURÍDICO DO CIBERCRIME NO BRASIL: UMA ANÁLISE DA VULNERABILIDADE DAS CRIANÇAS E ADOLESCENTES NO ESPAÇO VIRTUAL

Caroline Gassen Batistela<sup>1</sup>

Isadora Raddatz Tonetto<sup>2</sup>

### RESUMO

O presente artigo objetiva uma análise jurídica a respeito da cibercriminalidade, prática que tem se desenvolvido de forma crescente devido à apropriação que as pessoas passaram a fazer das tecnologias da informação e comunicação. Como estas espécies de criminalidade possuem características próprias e exigem maior conhecimento por parte dos seus autores, muitas vezes os órgãos do Estado se veem desafiados no seu combate, o que transmite uma falsa ideia de impunidade e incentiva a sua realização. Esta situação culminou, no Brasil, com a edição de leis, que prevêm alguns crimes informáticos, discutida no âmbito deste artigo, especialmente no que concerne a sua adequação e suficiência diante da cibercriminalidade. Percebe-se que seu texto, após ser analisado, mostra que a edição da lei brasileira ocorreu de maneira casuística e sem o necessário debate e envolvimento da sociedade, ademais se propõe discutir se referida lei ampara de forma suficiente crianças e adolescentes que estão cada vez mais vulneráveis no espaço cibernético.

**Palavras-Chave:** Internet. Cibercrime. Crianças. Adolescentes.

### ABSTRACT

This article aims at a legal analysis regarding cybercrime, a practice that has been developing in an increasing way due to the appropriation that people started to make of information and communication technologies. As these types of criminality have their own characteristics and require greater knowledge on the part of their perpetrators, State organs are often challenged in their fight, which conveys a false idea of impunity and encourages their realization. This situation culminated, in Brazil, with the enactment of laws, which provide for some computer crimes, discussed within the scope of this article, especially with regard to its adequacy and sufficiency in the face of cybercrime. It is noticed that his self-text, after being analyzed, shows that the edition of the Brazilian law occurred on a case by case basis and without the necessary debate and involvement of society, besides proposing to discuss whether that law sufficiently supports children and adolescents who are each increasingly vulnerable in cyberspace.

**Key-Words:** Internet. Cybercrime. Children. Teens.

<sup>1</sup> Advogada inscrita na OAB 102.718, Especializando em Direito de Família e Sucessões pela FMP. carolinebatistel@gmail.com

<sup>2</sup> Advogada inscrita na OAB 106.415, Especialista em Ciências Penais e Criminais pela FAPAS. isadorarad@hotmail.com

## INTRODUÇÃO

Sabe-se que as relações ocorridas na internet não se evadem do Direito, portanto, passíveis da incidência da atuação do Estado e das regras jurídicas vigentes. Cabe ao Direito, disciplinar e regulamentar os comportamentos que ocorrem também no ambiente virtual. Há poucos anos o Brasil editou a Lei nº 12.965/14, Marco Civil da Internet, que regula os crimes praticados em ambiente virtual. Referida lei, revela-se não só atrasada, mas insuficiente principalmente quanto a proteção de crianças e adolescentes.

Perante isso, questiona-se: É possível afirmar que a legislação brasileira, mostra-se suficientemente adequada para responder aos desafios da nova criminalidade, sendo um desses desafios a vulnerabilidade de crianças e adolescentes que se utilizam da tecnologia?

Para responder a este problema de pesquisa utilizou-se o método de abordagem dedutivo, pois a pesquisa partiu de uma abordagem geral de conceituação e identificação das normas punitivas para essa nova forma de crime, a partir de uma análise ampla da legislação brasileira com o objetivo de verificar especificadamente se referida norma apresenta efetivo grau de proteção aos que fazem parte da rede.

## 1 GLOBALIZAÇÃO E OS DESAFIOS DE COMBATER A CIBERCRIMINALIDADE

Com o mundo globalizado pressupõe-se que, as trocas e os contatos de informações, capitais, pessoas e conhecimentos são feitas em tempo real entre os estados, o que facilita a divulgação de dados, notícias e comunicações, mas também gera uma grande preocupação, pois com todo esse avanço intensifica-se a prática de delitos virtuais, que são praticados por meio da internet, ferramenta que amplia e aprofunda a globalização.

Para adaptar-se ao termo que dá origem a esse estudo, se faz necessário ter um conhecimento do que é a internet. Segundo a Portaria 148 do Ministério de Estado das Comunicações, de 31.05.1995, o qual aprovou a Norma 004/95, internet é o “nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores,

equipamentos e protocolos necessários à comunicação entre computadores, bem como software e os dados contidos nestes computadores” (BRASIL, 1995).

Já nas palavras de Zanellato, “A Internet é um suporte (ou meio) que permite trocar correspondências, arquivos, ideias, comunicar-se em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos”. Nesta senda pode-se dizer que a internet é uma rede de computadores interligados (ZANELATO, 2002).

A internet foi propagada e alavancada em vários países devido à rápida globalização, que além de trazer inúmeros benefícios, traz consigo seus malefícios, que vem norteando o cotidiano, se tornando comum na realidade atual. Um fato de suma importância da globalização foi à inserção do uso da internet no dia a dia das pessoas, com esse processo tal tecnologia não é mais um simples passa tempo, e torna-se a mais importante fonte de notícias, de comunicação, estreitando os laços, ampliando a vulnerabilidade diante de algumas situações.

Segundo Teixeira, o escritor e jornalista norte-americano Thomas Friedman, afirma que todos os avanços advindos com a globalização, fizeram surgir uma nova fase, a fase do mundo plano, que ele define da seguinte forma:

É uma nova fase da globalização, iniciada por volta de 2000, em que não apenas as empresas, mas também os indivíduos podem atuar em âmbito mundial. Isso se tornou possível graças algumas tecnologias revolucionárias - a internet, a telefonia celular, a rede de fibra óptica mundial. Elas criaram uma plataforma que permite múltiplas formas de comunicação, colaboração e inovação. Toda economia mundial se apoia nessa plataforma, que está achatando o mundo transformando todos nós em vizinhos. (TEIXEIRA, 2005).

Todo esse avanço dos meios de comunicação e das tecnologias incorporou-se à rotina atual, e é visto que essa mudança não passou despercebida aos olhos de alguns criminosos, pois ela veio acompanhada de ações indevidas as quais são praticadas por ação individual, bem como por membros de organizações criminosas, ensejando assim os delitos virtuais, que podem ser cometidos com uso de computador, tanto com a finalidade de atingir direitos de terceiros que também interagem no ambiente virtual, quanto com o objetivo de atacar os sistemas informáticos e os dados guardados no equipamento.

Os crimes virtuais podem ser conceituados como condutas que ocorrem de modo não autorizado a sistemas informáticos, comunicações telefônicas, dados pessoais e outros.

Ainda de forma abrangente, Mello define crime de informática como sendo toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão. (MELLO, 2012).

Nestas ações os infratores ludibriam as vítimas para obter vantagem financeira e pessoal, ou ainda para conseguirem dados particulares e usá-los em proveito próprio.

Esses crimes surgem ao decorrer desse meio evolutivo e ainda pouco regulado que consiste a internet, não podendo se afirmar que à medida que avança o crescimento da rede e a transferência de informação por meio dela, avance também um método protetivo aos usuários. O processo legislativo, por sua vez, deixa a desejar no momento em que não se torna bastante ágil comparado com a velocidade com que esses novos crimes acontecem e se multiplicam.

De acordo com essa reflexão, Marco Antônio Machado Ferreira de Melo afirma:

Esta nova era digital exige um processo legislativo ágil, capaz de acompanhar a evolução tecnológica e suas consequências sociais. Se é verdade que a solução jurídica precede a solução tecnológica, estamos literalmente desprotegidos. A solução jurídica pra questões das novas tecnologias, que evoluem rapidamente, não pode depender de um processo legislativo arcaico e moroso por natureza, concebido num outro tipo de sociedade pós-moderna. Há necessidade de adequação de nossa legislação para este novo momento. O Direito e a Ciência do direito estarão em permanente crise, decorrente da velocidade das transformações sociais, políticas e tecnológicas. (MELO, 2012)

Posicionando-se de acordo com o pensamento de Marco Antônio Ferreira de Melo, percebe-se a imensa dificuldade de combater tais crimes, não só pelos problemas de investigação que revelam, por serem velozes e muitas vezes despercebidos, mas também pela falta de legislação adequada.

Além do fato de não haver uma legislação adequada para combater esses ilícitos, a elevada tecnicidade e a forma especializada com que esses crimes são praticados fazem com que os dados a serem rastreados para solução desse problema sejam elevados, o que causa morosidade ao apurar os fatos.

De acordo com Maria José Morgado, são sete os obstáculos para o combate ao cibercrime:

1. A existência de uma multiplicidade de sistemas informáticos oficiais e das autoridades compartimentados.
2. Um quadro legal confuso do estilo manta de retalhos a potenciar dúvidas e impunidade.
3. Dispersão e sobreposição das várias autoridades competentes para o controlo do fenómeno.
4. Fragilidade dos esforços ao nível da prevenção.
5. Insuficiente atuação ao nível da repressão.
6. Falta de cooperação internacional refletida no funcionamento das estruturas nacionais.
7. Falta notória de recursos compatíveis com as exigências de contra-ataque do lado da PJ e do MP. (MORGADO, 2014)

Pelas palavras da autora percebe-se um claro descompasso entre a sofisticação dos criminosos e dos sistemas informáticos por eles utilizados e a estrutura do Estado, o que aponta para a necessidade de o ente estatal aprimorar seus instrumentos e lançar um novo olhar sobre a sociedade informacional. Tal é a evolução da internet e a ausência de normas que punam os ilícitos derivados dela que aumenta a vulnerabilidade das pessoas e dos bens diante desse novo contexto inaugurado pelo uso das tecnologias informacionais.

Em frente a toda essa onda de novos crimes e de outros tipos penais que se modificam pelo uso das tecnologias, em especial a Internet, torna-se evidente a necessidade de ações do Estado e da existência de normas que respondem satisfatoriamente a esse novo tipo de problema jurídico. Tal se mostra imperioso para a proteção aos internautas, segurança esta que deve estar presente no momento de dar e receber informações e em todas as interações no ambiente virtual.

Como já referido, a velocidade da produção legislativa não é a mesma empregada para a evolução das tecnologias e das novas possibilidades que seu uso revela aos internautas. Com isso muitas condutas que violam direitos e causam prejuízos econômicos aos usuários da Internet não são suficientemente tratadas, a exigir esforço legislativo e dos agentes de repressão. É sobre esse cenário que versará o próximo tópico, destinado a discutir a recente legislação brasileira destinada ao combate dos crimes virtuais.

## 2 A LEI DE CRIMES INFORMÁTICOS BRASILEIRA: SEU HISTÓRICO E ÂMBITO DE ABRANGÊNCIA

Sabe-se que as relações ocorridas na internet não se evadem do Direito, ou seja, não estão despregadas do contexto social e, portanto, são passíveis da incidência da atuação do Estado e das regras jurídicas vigentes. Cabe ao Direito, portanto, disciplinar e regulamentar os comportamentos que ocorrem no ambiente virtual, pois onde os atos de uns afetam bens jurídicos de outros se torna indispensável à existência de legislação para tentar evitar, minorar e, quando isso não for possível, punir as condutas que causarem danos.

A Carta Magna de 1988 versa em seu art. 5º XXXIX que “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, assim conclui-se que para punir um crime praticado por meio da internet, é necessário que se tenha uma norma adequada para o tipo penal.

As primeiras investidas legislativas ligadas à internet, vieram a ocorrer com o advento do Plano Nacional de Informática e Automação, Lei 7.232/84, que versava sobre diretrizes da informática no Brasil. Alguns anos depois, foi sancionada a Lei nº 9609/98, sendo está a primeira a versar e descrever as infrações de informática, da qual se faz referência de alguns artigos:

Art. 12. Violar direitos de autor de programa de computador:

Pena – Detenção de seis meses a dois anos ou multa.

§ 1º Se a violação consistir na reprodução, por qualquer meio, de programa de computador, no todo ou em parte, para fins de comércio, sem autorização expressa do autor ou de quem o represente:

Pena – Reclusão de um a quatro anos e multa.

§ 2º Na mesma pena do parágrafo anterior incorre quem vende, expõe à venda, introduz no País, adquire oculta ou tem em depósito, para fins de comércio, original ou cópia de programa de computador, produzido com violação de direito autoral. § 3º

Nos crimes previstos neste artigo, somente se procede mediante queixa, salvo:

I – quando praticados em prejuízo de entidade de direito público, autarquia, empresa pública, sociedade de economia mista ou fundação instituída pelo poder público;

II – quando, em decorrência de ato delituoso, resultar sonegação fiscal, perda de arrecadação tributária ou prática de quaisquer dos crimes contra a ordem tributária ou contra as relações de consumo.

§ 4º No caso do inciso II do parágrafo anterior, a exigibilidade do tributo, ou contribuição social e qualquer acessório, processar-se-á independentemente de representação. (BRASIL, 1998)

O exame desses dispositivos indica que o escopo da referida Lei não tinha o alcance necessário para conter novas formas de criminalidade, como roubo de dados pessoais, de senhas e outros neste mesmo diapasão. Neste interim, surgiram outros projetos de lei que versavam sobre os crimes cometidos na rede. No longínquo ano de 1999, surgiu o projeto da Lei Azeredo (PL 84/99), cujo objetivo era definir crimes cibernéticos, bem como criar alguns tipos, tais como: *hackear* o computador de alguém, difundir vírus, derrubar sites, repassar pornografia infantil, dentre outros que ocorriam no momento. Outros projetos de lei foram incluídos na Lei Azeredo – como o estelionato eletrônico (*phishing*) – e em 2003 ela foi aprovada pela Câmara. No Senado, ele também tramitou por um longo tempo, onde foi reformulado até chegar à sua versão final em 2008. (VENTURA, 2012).

Por se tratar de um projeto de lei um tanto polêmico, pois restringia amplamente a privacidade e liberdade na internet, a Lei Azeredo teve 17 dos seus 23 artigos removidos, o que fez com que esta proposta não versasse mais sobre invasão de computadores ou redes, divulgação de informações sigilosas e afins.

Somente em 2012 que a Legislação brasileira passou a contar, no que diz respeito aos cibercrimes, com uma lei mais específica sobre as invasões de computadores. Em 2012 a Presidente Dilma Rousseff sancionou as Leis 12735 e 12737, que tipificam os crimes eletrônicos no País. A partir de então, invadir ou adulterar computadores, criar programas que permitam violar sistemas e divulgar dados obtidos sem autorização pode resultar multa e aplicação de pena privativa de liberdade. (DIAS, 2012).

Na visão de Leonardo Sica:

Trata-se de lei casuística e promocional. Casuística porque a sua edição foi motivada em um caso concreto, distanciando-a dos requisitos da abstração e generalidade, que devem informar as boas leis. Promocional, porque a enorme repercussão do caso concreto permitiu ao parlamento, mais uma vez, legitimar-se por meio do discurso de lei e ordem e também abriu espaço para profissionais do direito que se especializaram como porta vozes do “direito digital”, com a indisfarçável intenção de se apropriar dessa parcela do mercado de trabalho (SICA, 2012).

Leonardo Sica é realista ao falar que a lei é casuística e promocional, pois sua rápida tramitação deveu-se ao alvoroço causado pela mídia. A repercussão dos fatos fez com que o

Poder Legislativo e alguns especialistas criassem um discurso de ordem, talvez uma tentativa de se autopromoverem, para que pudessem mostrar trabalho eficiente à sociedade, editando uma lei. O fato de essa edição ter se dado às pressas pode trazer falhas por não ter sido devidamente estudada e debatida com a sociedade.

Essa posição mais crítica à existência de lei penal sobre a matéria e, especialmente sobre a sua rápida tramitação, não é partilhada por todos os doutrinadores, pois para Auriney Brito:

Apesar de ter sido criada sob a cinematografia da mídia, as novas leis de crimes informáticos não estão em desequilíbrio holístico, pois, vem a satisfazer grande parte das necessidades de criminalização de condutas intoleráveis na Sociedade da Informação. (BRITO, 2013).

Embora haja inúmeras opiniões sobre esta lei, deve-se dizer que a referida legislação dispõe sobre a tipificação de delitos praticados via internet, estabelecendo uma responsabilização aos infratores, o que até então não estava especificado no Código Penal Brasileiro.

A Lei Dieckmann restaurou alguns dos dispositivos da Lei Azeredo, porém sem às polêmicas da proposta anterior. A lei vigente criminaliza quem divulga informações reservadas obtidas por meio ilícito, como invasão, e quem dá suporte para isso, como também era previsto no Projeto Azeredo. No entanto, agora essa tipificação é feita com uma linguagem menos abrangente e de forma mais precisa, característica que se torna imprescindível, já que o Direito Penal não pode ser amplo, já que tem como princípio norteador o da mínima intervenção ou “*ultima ratio*”. Assim, o Direito Penal estando legitimado para incidir quando os demais ramos do Direito se mostrarem incapazes ou insuficientes para a proteção dos bens jurídicos.

Não deve o Direito Penal ser o primeiro e único instrumento de controle social, já que sua aplicação deve ser subsidiária, sendo deste modo a última alternativa, a *última ratio*.

Um dos princípios norteadores do Direito Penal é o da intervenção mínima que orienta e limita o poder penal violento do Estado, e para que seja aplicado faz-se necessário o esgotamento de todos os meios extrapenais de controle social existentes. A fragmentariedade e a subsidiariedade são duas características do Direito Penal que se relacionam com o princípio da intervenção mínima.

Assim, percebe-se que a intervenção mínima está inteiramente ligada à doutrina do minimalismo penal, que apregoa a não utilização deste ramo do Direito como a primeira forma de resolução de conflitos. A opção por outras áreas do Direito e pela adoção de formas distintas de intervenção jurídica se justifica em virtude da forma violenta e rigorosa com que atua o Direito Penal para manter a ordem social, o que determina que este ramo do Direito seja usado de forma subsidiária e fragmentado.

Ainda que a Lei nº 12.737/2012 trouxesse algumas respostas desejadas pela população, ela ainda deixava a desejar, e se mostrava ampla, ambígua e ineficaz diante do cenário cibernético. Deste modo em 2014 foi instaurado o Marco Civil da Internet, diante a promulgação da Lei 12.965/2014.

O primeiro capítulo da Lei 12.965/14 traz algumas disposições preliminares acerca da regulamentação do uso e funcionamento da internet no Brasil, estabelecendo alguns princípios capazes de proteger os usuários, que deverão servir de referências para a elaboração de outros diplomas legais referentes a internet.

O Marco Civil da Internet, também chamado de Constituição da Internet, foi moldado com base em três fundamentos essenciais, a neutralidade, a privacidade e a fiscalização.

A neutralidade tem como função principal coibir ações abusivas das empresas que prestam serviços de internet, telefonia e afins. O princípio da privacidade é a garantia da inviolabilidade das comunicações dos usuários, assim a lei atribui que deve haver sigilo das informações do usuário ao provedor do recurso de internet, e por fim a fiscalização dos acessos.

A Lei do Marco Civil da Internet em seu artigo 2º, II, dispõe que além da liberdade de expressão, o uso da internet no Brasil também tem como fundamento os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais. (BRASIL, 2014).

A Constituição de 1988 consagrou os direitos humanos como um dos pilares do ordenamento jurídico brasileiro. (BRASIL, 1988).

Na definição trazida pela Organização das Nações Unidas (ONU), entende-se por direito humanos “garantias jurídicas universais que protegem indivíduos e grupos contra

ações ou omissões dos governos que atentem contra a dignidade humana.” (TAVARES, 2015).

Percebe-se a íntima ligação dos Direitos Humanos com a dignidade da pessoa humana, a para melhor compreensão, se faz necessário o uso das palavras de Kildare Gonçalves de Carvallho:

A dignidade da pessoa humana significa ser ela, diferentemente das coisas, um ser que deve ser tratado e considerado como um fim em si mesmo, e não para obtenção de algum resultado. A dignidade da pessoa humana decorre do fato de que, por ser racional, a pessoa é capaz de viver em condições de autonomia e de guiar-se pelas leis que ela própria edita: todo homem tem dignidade e não um preço, como as coisas, já que é marcado, pela sua própria natureza, como fim em si mesmo [...] (CARVAVALHO, 2008, p. 693).

Veja que o Marco Civil da Internet traz os direitos humanos como um de seus fundamentos, busca saber se o compilado de artigos por ele trazidos é capaz de assegurar a dignidade das crianças e adolescentes que fazem uso da rede.

### **3 A VULNERABILIDADE DAS CRIANÇAS E ADOLESCENTES NO ESPAÇO VIRTUAL**

É de suma importância esclarecer o conceito de criança e adolescente segundo o Estatuto da Criança e do Adolescente, que descreve as faixas etárias que definem e diferenciam crianças e adolescentes.

Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade.  
Parágrafo único. Nos casos expressos em lei, aplica-se excepcionalmente este Estatuto às pessoas entre dezoito e vinte e um anos de idade. (BRASIL, 1990)

Salienta-se que o Brasil adaptou sua legislação com base em tratados e convenções, seguindo as diretrizes de âmbito internacional, sobre Direitos Humanos e Direito da Criança. Enfatizando-se assim a proteção aos direitos à liberdade, à dignidade, à inviolabilidade da integridade física, moral e psíquica das Crianças e Adolescentes.

Com o já referido avanço das tecnologias e sua precoce inserção no cotidiano das pessoas, os usuários do mundo virtual vem diminuindo de idade cada vez mais, em contrapartida a instrução das pessoas que se utilizam dessas ferramentas ainda é extremamente baixo, seja pelo pouco nível de escolaridade, pela idade precoce, ou até a falta da informação, não possuem o conhecimento dos perigos que cercam toda essa tecnologia.

Se adultos, já são vítimas de inúmeros crimes cometidos através da rede, como proteger uma criança ou adolescente nesta seara tão obscura. As oportunidades que se dá aos cibercriminosos quando se negligencia aos cuidados com a vida digital infantil pode trazer danos irreparáveis as vítimas, e aqui não se faz menção somente a pedofilia, mas ao crime em constante ascensão nas redes, o cyberbullying que tem levados inúmeras vítimas ao suicídio.

É dever legal dos pais educar os filhos, e esse princípio não deve ser negligenciado também nas relações virtuais. A Constituição Federal prevê esse dever em seu artigo 229, o qual preceitua que “os pais têm o dever de assistir, criar e educar os filhos, e os filhos maiores têm o dever de ajudar e amparar os pais na velhice, carência ou enfermidade”. (VOZES, 2019).

Dito isso, é de extrema importância que a educação digital seja pauta nos núcleos familiares atuais, pois assim como se deixa uma criança livre para usar e dispor de redes sociais e um vasto conteúdo oferecido pela internet, deve-se em contrapartida haver uma supervisão parental, segura e continua, no que tange aos limites e principalmente aos danos que este universo pode causar.

No contexto do Marco Civil da Internet foi dada atenção ao conteúdo acessado por crianças e adolescentes nas redes, visto que é dever fundamental do Estado proteger crianças e adolescentes, mas também deve-se levar em consideração o dever de atuação de pais e responsáveis na proteção de seus filhos no ambiente virtual.

O Marco Civil da Internet traz em seu artigo 29 a possibilidade de monitoramento das atividades das crianças e adolescentes na rede.

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente. Parágrafo único. Cabe ao poder público, em conjunto com os

provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no caput, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes. (BRASIL, 2014).

Referido artigo permite que pais e responsáveis usem programas de computadores para tutelar o ambiente virtual acessado por seus filhos, monitorando e controlando o conteúdo que acessam. No entanto esse controle deve obedecer algumas limitações impostas pelo Estatuto da Criança e do Adolescente, e é neste ponto que a Constituição da Internet, começa falhar quando de trata de proteger crianças e adolescentes dos riscos virtuais.

No artigo 100 do referido estatuto resta claro que:

Art. 100. Na aplicação das medidas levar-se-ão em conta as necessidades pedagógicas, preferindo-se aquelas que visem ao fortalecimento dos vínculos familiares e comunitários. (BRASIL, 1990).

Deste modo, fica expresso que toda e qualquer medida tomada pelos pais deve levar em consideração as necessidades pedagógicas, que ao mesmo tempo fortaleçam os laços familiares. Assim sugere o estatuto que neste caso os pais e responsáveis devem usar uma mediação pautada na educação, na conversa, ensinando aos seus filhos os riscos trazidos pela internet, como se prevenir, e como agir, caso algo ocorra.

É certo que essa medida em nada protege crianças e adolescentes, muitas vezes por não atentarem aos que os pais falam e ensinam, como também pelo instinto curioso que os guiam.

Outro dispositivo que se choca ao Marco Civil da Internet é o inciso V do mesmo artigo, que relata:

V - privacidade: a promoção dos direitos e proteção da criança e do adolescente deve ser efetuada no respeito pela intimidade, direito à imagem e reserva da sua vida privada (BRASIL, 1990).

Monitorar ou Co-utilizar as redes virtuais podem ser consideradas praticas abusivas pelo Estatuto da Criança e do Adolescente, vez que invadem o respeito à intimidade, à imagem e a reserva da vida privada.

O direito à privacidade é um direito fundamental previsto na Constituição Federal de 1988. Diz o artigo 5º, inciso X, que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. Dessa forma, a privacidade da criança e do adolescente é um direito inerente, não podendo os pais violá-los, por tratar-se de um direito fundamental.

Sabe-se que os direitos fundamentais, no entanto não são absolutos. Em situações que haja conflitos entre direitos fundamentais, deve ser analisada sua proporcionalidade. No caso da privacidade da criança e do adolescente, este entra em conflito com o disposto no artigo 227 da Constituição Federal, o dever da família de proteção da criança e do adolescente contra qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Nas palavras de Virgílio de Afonso:

Boa parte daquilo que a doutrina e jurisprudência muitas vezes tomam como dado é, na verdade produto dessa simples divisão teórica entre o direito em si e suas restrições. É principalmente a partir dessa distinção que se pode chegar ao sopesamento como forma de solução das colisões entre direitos fundamentais e, mais que isso, à regra da proporcionalidade, com suas três sub-regras – adequação, necessidade e proporcionalidade em sentido estrito. Isso porque é somente a partir do paradigma da teoria externa – segundo o qual as restrições, qualquer que seja sua natureza, não tem qualquer influência no conteúdo do direito, podendo apenas, no caso concreto, restringir seu exercício – que se pode sustentar que, em uma colisão entre princípios, o princípio que tem de ceder em favor de outro não tem afetadas sua validade e, sobretudo, sua extensão prima facie. (SILVA, 2011, p. 138)

A violação da privacidade da criança e do adolescente como forma de proteger e tutelar sua proteção integral, deve ser feita de forma proporcional. A violação não extingue o direito a privacidade, mas limita seu exercício na medida que se faz necessária e contundente para a proteção na rede.

Desta forma, o Art. 29 do Marco Civil da internet não oferece uma efetiva proteção as crianças e adolescente, no momento em que surge a possibilidade de pais e responsáveis ofenderem o direito a privacidade destes, ao usarem programas para o exercício do controle parental.

Importante salientar que o mecanismo apenas abre uma possibilidade dos pais protegerem seus filhos de conteúdos possivelmente danosos, mas em nenhum momento refere-

se a possibilidade de fiscalização de e-mails, contas em redes sociais, conversas provadas e afins. É importante que essas restrições ocorram na proporção que sejam necessárias, para que também não ocorra um abuso excessivo e desnecessário por parte dos pais.

A função da autoridade parental é favorecer o desenvolvimento da personalidade da criança, do jovem e do adolescente. Para tanto, como já mencionado, compete aos pais prover seus filhos de afeto, cuidado, educação, cultura, saúde e assistência moral e material, devendo sempre observar o princípio constitucional do melhor interesse da criança. (CRUZ, 2010).

O artigo 29 em seu parágrafo único traz ainda a determinação de que o poder público e sociedade civil têm o dever de fornecer a todos informações sobre o correto uso de tais programas, sendo que estes devem ser utilizados em conjunto com boas práticas para a inclusão digital de crianças e adolescentes.

Verificado que as situações de perigo no âmbito digital precisam, sempre, ser detectadas; impõe-se, para a tutela integral de proteção dos filhos, o dever de controle das suas interatividades virtuais, sob pena de aperfeiçoar-se a negligência parental com a devida responsabilização civil. Do contrário, crianças e adolescentes aparentemente sozinhas em seus quartos, virtualmente conviverão com estranhos e com os perigos, enquanto estarão, em verdade, sozinhas dentro da família.

## CONSIDERAÇÕES FINAIS

Diante do exposto pode-se afirmar que a Legislação Brasileira no que diz respeito a cibercriminalidade ainda é muito recente e embora haja projetos antigos, como o da Lei 7.232/84 e a Lei Azeredo, é somente no ano de 2012 E 2014 que as leis passam a ser mais elaboradas.

A Lei 12.737 de 2012, posta em debate no item 2 do presente artigo, mostra a imaturidade brasileira em se aprovar uma lei casuística às pressas, motivada por um caso de grande repercussão na mídia, o qual exigia uma solução ao problema. Neste teor, é indiscutível

que a lei apresentada, por não ter sido devidamente debatida e estudada, trouxe consigo inúmeras falhas.

O interesse de mostrar resposta à sociedade para a cena que repercutia na mídia envolvendo uma atriz global era tamanho que o Poder Legislativo não ponderou o uso de princípios fundamentais do Direito, tais como o princípio do minimalismo penal e da intervenção mínima. Ao contrário disso, buscou respaldo do Direito Penal em detrimento de outras soluções, o que é criticável, pois este ramo do Direito deve ser a última forma de resolução para estes conflitos emergentes na sociedade em rede. Aliado a isso, revela-se lacunosa porque não previu importantes estratégias, como a cooperação internacional, necessária em se tratando de crimes que envolvem o uso de tecnologias da informação e comunicação que, como trabalhado na primeira parte deste artigo, ultrapassam as fronteiras estatais.

Quanto ao Marco Civil da Internet, este nada mais é do que uma consequência decorrente da evolução legislativa associada aos meios de comunicação no espaço cibernético da era digital.

Era necessária uma legislação robusta sobre o assunto, ocorre que a maioria das leis editadas ainda se mostram lacunosas e falhas.

As medidas de proteção de Crianças e Adolescentes neste cenário são de suma importância. O papel dos pais por meio da mediação é essencial para protegê-los, o diálogo, é sempre o primeiro e mais importante caminho para evitar que abusos aconteçam.

Porém, as medidas restritivas e o monitoramento, são essenciais no combate aos perigos virtuais, diminuem a vulnerabilidades destes perante a rede, porém tais medidas podem esbarrar no Estatuto da Criança e do Adolescente.

Com medidas legislativas pontuais e uma presente atuação dos pais e responsáveis, a utilização da internet pode se dar de maneira segura, contribuindo para o desenvolvimento pessoal das Crianças e Adolescentes. Ao conciliar a proteção integral, respeitando o direito à privacidade, tem-se o aumento da participação do jovem na rede de forma benéfica e sadia, sem prejuízos aos seus direitos e acima de tudo sem risco. Uma solução possível, mas ainda arriscada, seria a implementação de artigos determinados no Código Penal, bem como no

Estatuto da Criança e do Adolescente, dispendo sobre condutas e punições nos casos específicos.

## REFERÊNCIAS

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Presidência da República, 1988. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicaocompilado.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm). Acesso em: 15 ago. 2020.

BRASIL. **Lei nº 9.609 de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/19609.htm](http://www.planalto.gov.br/ccivil_03/leis/19609.htm). Acesso em: 12 ago. 2020.

BRASIL. **Lei 12.965 de 23 de abril de 2014**. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 24 abr. 2014. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 12 ago. 2020

BRASIL. **Lei n.8.069 de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/leis/18069.htm](http://www.planalto.gov.br/ccivil_03/leis/18069.htm). Acesso em: 10 ago. 2020.

BRASIL. **Lei n. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2014/lei/112965.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm). Acesso em: 13 ago. 2020

BRITO, Auriney. **Análise da Lei 12.737/12 – “Lei Carolina Dieckmann**. 2013. Disponível em: <http://atualidadesdodireito.com.br/aurineybrito/2013/04/03/analise-da-lei-12-73712-lei-carolina-dieckmann/>. Acesso em: 16 ago. 2020.

CARVALHO, Kildare Gonçalves. **Direito Constitucional: teoria do estado e da constituição e direito constitucional positivo**. 16. ed. Belo Horizonte: Del Rey, 2010.

CRUZ, Elisa Costa. **O direito dos filhos à privacidade e sua oponibilidade à autoridade parental**. 2012. Disponível em: <https://www.ibdfam.org.br/artigos/798/O+direito+dos+filhos+%C3%A0+privacidade+e+sua+oponibilidade+%C3%A0+autoridade+parental> Acesso em: 16 ago. 2020.

DIAS, Tatiana de Mello. **Dilma sanciona leis que definem cibercrimes**. 2012. Disponível em: <http://blogs.estadao.com.br/link/tag/lei-azeredo/>. Acesso em: 12 ago. 2020.

MELO, Marco Antônio Machado Ferreira de. A tecnologia e a solidariedade. *In*: ZANIOLO, Pedro Augusto. **Crimes Modernos: o impacto da tecnologia no direito**. 2. ed. Curitiba: Juruá, 2012.

MORGADO, Maria Jose. **Os sete obstáculos de combate ao cibercrime**. 2014. Disponível em: <http://oscot.pt/os-sete-obstaculos-no-combate-ao-cibercrime>. Acesso em: 12 ago. 2020.

SICA, Leonardo. **Lei Carolina Dieckmann: aspectos penais**. 2012. Disponível em: <http://www.cartaforense.com.br/conteudo/artigos/lei-carolina-dieckmann--aspectos-penais/11242>. Acesso em: 12 ago. 2020.

SILVA, Virgílio Afonso da. **Direitos fundamentais: conteúdo essencial, restrições e eficácia**. 2. ed. São Paulo: Malheiros, 2011.

TAVARES, Raquel. **O que são direitos humanos?** Gabinete de Documentação e Direito Comparado, 2015. Disponível em: <http://direitoshumanos.gddc.pt/IPAG1.htm>. Acesso em: 14 ago. 2020.

TEIXEIRA, Jerônimo. Achatando o Globo. **Veja**, São Paulo, v. 38, n. 50, dez. 2005.

VENTURA, Felipe. **Dieckmann x Azeredo: como se comparam os dois projetos de lei para crimes virtuais**. 2012. Disponível em: <http://gizmodo.uol.com.br/projeto-leis-dieckmann-azeredo/>. Acesso em: 14 ago. 2020.

VOZES, Gazeta do Povo. **Monitoramento dos pais na internet X invasão de privacidade?** 2015. Disponível em: <https://www.gazetadopovo.com.br/vozes/direito-e-tecnologia/monitoramento-dos-pais-na-internet-x-invasao-de-privacidade/>. Acesso em: 10 ago. 2020.

ZANELLATO, Marco Antonio. Condutas Ilícitas na sociedade digital, **Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo**, Direito e Internet, São Paulo, n. 4, jul. 2002.