

EXPLORAÇÃO SEXUAL INFANTOJUVENIL NA INTERNET E A PROTEÇÃO ÀS CRIANÇAS E AOS ADOLESCENTES

Denise Casanova Villela*

Resumo: Este artigo visa a abordar o tema da exploração sexual infantojuvenil na internet sob o aspecto da proteção da criança e do adolescente à luz da legislação nacional, especialmente o Estatuto da Criança e do Adolescente, Lei nº 8.069, de 13 de junho de 1990; a Lei do Marco Civil da Internet, Lei nº 12.965 de 23 de abril de 2014 e a lei que estabelece o sistema de garantias de direitos da criança e do adolescente vítima e testemunha de violência, Lei nº 13.431 de 4 de abril de 2017, que disciplina a escuta especializada e o depoimento especial. Aponta algumas dificuldades na aplicação da legislação pátria, no que tange à proteção da infância e adolescência, e sugere alguns encaminhamentos para que os princípios da proteção integral e a prioridade absoluta preconizados na Constituição Federal e Estatuto da Criança e do Adolescente sejam realmente efetivos. Indica, ainda, sugestões de proteção das vítimas.

Palavras-chave: Exploração sexual infantojuvenil na internet. Escuta especializada de criança e adolescente em crimes cibernéticos. Riscos da internet para crianças e adolescentes. Crimes cibernéticos contra crianças e adolescentes.

* Promotora de Justiça. Coordenadora do Centro de Apoio da Infância, Juventude, Educação, Família e Sucessões do Ministério Público do Rio Grande do Sul. Graduada em Ciências Jurídicas e Sociais pela Universidade Federal do Rio Grande do Sul. Mestre pela *Cumberland School of Law*. Samford University/US. Curso de extensão técnica de coleta de testemunho adulto e infantil. Pró-reitoria de extensão da PUCRS e MPRS, Porto Alegre. Curso de extensão em técnicas de entrevista com suspeitos e detecção de mentiras. Pró-reitoria de extensão da PUCRS. Faculdade de Psicologia. Porto Alegre. Curso de Educação Continuada: Treinamento em técnicas de entrevista com testemunhas e vítimas – módulo I. Pró-reitoria de extensão da PUCRS, Faculdade de Psicologia, Porto Alegre. Curso de extensão e análise da credibilidade do testemunho. Pró-reitoria de extensão da PUCRS, Faculdade de Psicologia, Porto Alegre. Treinamento de Combate a Crimes de Pedofilia pela Internet, ministrado pela International Center for Missing & Exploited Children, FBI-US. Curso de Investigadores de Delitos contra Menores em América Del Sur – Interpol – Oficina Regional Buenos Aires, Argentina e ICMEC. Curso sobre “Judicialización de casos de Trata de Persona” – Interpol – Oficina Regional Buenos Aires, Argentina. Curso de Inverstigadores de Explotación em Línea – Interpol – Oficina Regional Buenos Aires, Argentina.

Abstract: This article aims to approach the issue of child and adolescent sexual exploitation on the Internet under the protection of the children and adolescents in the light of national legislation, especially the Statute of the Child and Adolescent, Law No. 8.069, of June 13, 1990; the Civil Registry Law of the Internet, Law No. 12,965 of April 23, 2014 and the law establishing the system of guarantees for the rights of the children and adolescents, victims and witnesses of violence, Law No. 13.431 of April 4, 2017, which discipline specialized listening and special testimony. It points out some difficulties in the application of the country's legislation regarding the protection of the children and adolescents and suggests some routing so that the principles of the integral protection and the absolute priority advocated in the Federal Constitution and Statute of the Child and the Adolescent are really effective. It also gives suggestions in order to protect the victims.

Keywords: Child and adolescent sexual exploitation on the internet. Specialized listening of children and adolescents in cyber crimes. Internet risks for children and adolescents. Cyber crimes against children and adolescents.

Introdução

Com a modernidade e o avanço tecnológico, diversas questões vêm gerando discussões no campo ético e jurídico, principalmente no que se refere à proteção de crianças e adolescentes e sua exposição cibernética. Para aprofundar o tema é importante conhecer o ambiente denominado internet, onde podem ocorrer situações que envolvam violações de direitos, especialmente de crianças e adolescentes.

A palavra internet tem origem inglesa e significa rede internacional de computadores. Essa rede é interligada por linhas telefônicas, fibra ótica e satélites possibilitando o acesso a dados em qualquer lugar do mundo, conectando milhões de pessoas em redes de relacionamento que navegam pelas informações disponíveis no espaço virtual, chamado de *ciberespaço*. Surgiu em 1993, deixando gradativamente de ser utilizada apenas pelos governos e acadêmicos, passando a estar presente em diversos segmentos privados, inclusive nas residências. Com o tempo, outros equipamentos começaram a acessar essa rede, fazendo com que as informações fossem trocadas com maior facilidade e rapidez.

A internet tornou-se um fenômeno, uma vez que, através dela as pessoas têm a possibilidade de obter toda a sorte de informações sobre qualquer assunto, em qualquer lugar do mundo, além de permitir transferências de dados por meio de uma variedade de recursos e serviços como *e-mails*, comunicações instantâneas, compartilhamento de arquivos de música, fotos e filmes, redes sociais, aplicativos, etc.

Enfim, a rede mundial de computadores e outros equipamentos são fontes inesgotáveis de informações. Ao longo dos anos, foram criados sites de procura, buscando facilitar a troca de conhecimentos. Entretanto, trata-se de um espaço

público e, em razão disso, deve-se ter muita atenção e cuidado ao navegar na rede, para que sejam aproveitadas todas as possibilidades de obtenção de dados e informações, de forma segura.

O acesso à internet pode ser obtido utilizando-se diversos equipamentos, não apenas o computador, e os dados podem ficar gravados no aparelho ou em outros dispositivos, inclusive na conhecida pasta de armazenamento de dados, denominada *nuvem*. Isso faz com que a cautela na utilização desta ferramenta deva ser redobrada. Com o passar dos anos, novas normas têm sido editadas para a regulamentação do uso da Internet, com a finalidade de oferecer maior proteção e segurança aos direitos dos usuários.

Ao mesmo tempo em que essa rede passou a ser um produto essencial, como fonte inestimável de conhecimento e de troca de informações, também sobreveio sua utilização para a prática de diversos ilícitos. E quanto mais ela evolui tecnicamente, maior é a possibilidade de o usuário estar vulnerável ao acessá-la, pois a internet comporta diversos aplicativos, que vão sendo atualizados e modernizados com o tempo, por vezes se extinguindo, dando lugar a outros que surgem oferecendo maiores vantagens ao usuário. Esses aplicativos podem transmitir mensagens, imagens, vídeos, podem compartilhar os dados entre duas pessoas ou contas, ou, ainda, dividir as informações em grupos. Os dados compartilhados podem estar criptografados e até desaparecerem em questão de segundos. Essas características podem acarretar tratamentos diferenciados perante a legislação, inclusive com relação às atribuições e às competências para processar e julgar os casos de violações de direitos ocorridos na rede.

Uma das características da internet é a transnacionalidade, eis que, em princípio, uma vez posta a informação na rede mundial de computadores ela pode ser acessada por qualquer pessoa, em qualquer lugar no mundo. Entretanto, isso nem sempre acontece, porque alguns aplicativos e serviços disponíveis transmitem informações, ponto a ponto, envolvendo apenas os usuários do aplicativo, como, por exemplo, o *WhatsApp* e o *e-mail*. Porém, a situação não é tão simples, já que existem aplicativos que admitem a criação de grupos e, neste caso, os integrantes podem acessar o sistema em vários lugares no mundo. Assim, as questões que envolvem violações de direitos na internet estão longe de serem questões de fácil solução; pelo contrário, estão permeadas de pequenos detalhes que devem ser avaliados para que a prestação jurisdicional e a efetiva proteção sejam garantidas. A investigação, neste sentido, torna-se importante, para fins de fixação de competência no processamento das questões, na medida em que, caso comprovada a transnacionalidade, a atribuição e a competência para a investigação e judicialização dos fatos ocorridos na Internet pertencem à área federal, especialmente quando se tratar da área criminal.

Neste contexto, é importante que alguns conceitos sejam efetivamente conhecidos.

1 **Surface Web e Deep Web**

Não há a intenção de se esgotar o tema, mas passar alguns conceitos gerais, para a compreensão das dificuldades do enfrentamento das questões que envolvem a exploração sexual infantojuvenil na internet.

Surface Web é a rede que normalmente é utilizada pela maioria dos usuários da internet. Nela os dados são transformados em pacotes e enviados de um equipamento para outro utilizando linhas telefônicas ou banda larga, este último através de um provedor. Tudo que circula na *surface web* recebe um protocolo de acesso, que se chama IP (*internet protocol*), que é um número necessário para identificar a origem e o destino da informação, estabelecendo a direção do acesso. Esse protocolo é único¹ e não admite falsificação.

Isso dá segurança ao usuário, pois a existência do número de protocolo permite rastrear os contatos ocorridos na internet.

Tudo que diz respeito a e-mails, fotos e vídeos necessita de dois indicadores (de IP/TCP) para possibilitar a identificação da direção e localização do usuário.

Embora a internet pareça segura, com sua expansão, os números de protocolos podem ser compartilhados (IPV4 e IPV6).² Isso significa que uma mesma direção pode estar sendo compartilhada por vários usuários, tornando-se mais difícil a localização da direção dos dados e, conseqüentemente, do usuário. Nestes casos é importante que se conheçam as datas e horas de acesso, para que se tenha a segurança de apontar qual usuário estava acessando determinado conteúdo naquele momento.

A *Surface Web* presta serviços como *www (world wide web)*, *e-mails*, hospedagem e compartilhamento de arquivos (P2P), mensagens, *chat*, redes sociais, *voip (voice over ip)*, *e-commerce*.

A *deep web* ou *dark web*, por sua vez, de regra é conhecida como o lado obscuro da internet. É chamada assim, em razão de seu conteúdo e por não ser possível acessá-la através dos navegadores comuns (como *Firefox*, *Explorer* e *Chrome*), os quais só encontram sites na *surface web*.

Na *deep web* rodam programas como, por exemplo, a rede TOR (*The Onion Router*), que é representada pela imagem de uma cebola. Quando se entra em um site pela *surface web* é o computador de alguém que se comunica diretamente com o computador de outrem. Mas quando a rede TOR é utilizada, a comunicação vai passando por uma série de computadores aleatoriamente, os quais também estão conectados na rede, até chegar ao seu destino, tornando a

¹ BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Roteiro de atuação: crimes cibernéticos / 2. Câmara de coordenação e revisão. 3. es. rev. e ampl. Brasília: MPF, 2016. p. 27-29.

² *Ibidem*, p. 30-31.

rede TOR quase anônima. A quantidade de conteúdo que circula na *deep web* através das redes como TOR, *freenet*, I2P, dentre outras, é superior a tudo que se conhece, e ela contém de tudo, inclusive coisas ilegais, como manuais de guerra, tráfico de pessoas, terrorismo, pedofilia, comportamentos psicóticos, comércio ilegal de drogas e armas, e até sites para a contratação de assassinos.³ Mas, também contém vasta lista de livrarias de *e-books*, hospedagem gratuita, e muito conteúdo sobre qualquer coisa. Os domínios usados na rede TOR são com o sufixo “.onion”, ao invés de “.com”, “.com.br” ou “.net”, naturalmente usados na *surface web*. A compra e venda de bens e serviços são feitas através de uma moeda cibernética conhecida por *bitcoin* (*cybercurrebcy*). Trata-se de uma criptomoeda, cujo sistema de pagamento online é baseado em protocolo de código aberto, que é independente de qualquer autoridade central.⁴ Existe várias criptomoedas circulando na internet, não apenas a *bitcoin*, sendo elas utilizadas em um comércio que cresce vertiginosamente.

2 Exploração Sexual infantojuvenil na internet

A internet, hoje essencial para quase todas as atividades é utilizada muitas vezes de forma inadequada e até criminosas; por intermédio dela é realizada a propagação de pornografia infantil e juvenil, causando danos imensuráveis a milhares de crianças e adolescentes ao redor do mundo. Isso acontece em razão de alguns fatores, como por exemplo a disponibilidade, abundância, virtualização, anonimato, inteligência e ajuda entre pares, além do acesso fácil às crianças e aos adolescentes.⁵

O fato da inexistência de contato físico entre os usuários facilita com que crimes desta natureza sejam praticados, pois o agressor se esconde atrás do anonimato para praticar ilícitos, privilegiando-se diante da dificuldade de ser identificado.

O tráfego de exploração sexual infantil ao sob o aspecto global atingiu níveis alarmantes, segundo informações da Interpol. Em razão disso, em 2011, a Assembleia Geral da Interpol expediu a resolução nº AG-2011-RES-08 reco-

³ LAZARO, FERNANDES. Coordenador Forense Digital. Ferramentas e servicios del complejo mundial para La Innovaction – Complejo Mundial para La innovaction de INTERPOL. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires, Argentina, em 11 de junho de 2015.

⁴ Ibidem.

⁵ MACNAMARA, Maximiliano. Analista de la Subdirección de trata de Personas y Explotacion Infantil de INTERPOL. Las herramientas y servicios de INTERPOL para combatir la explotacion sexual infantil em línea. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires, Argentina, em 11 de junho de 2015.

mendando aos países membros, em relação ao abuso infantil, que estabeleça uma investigação sistemática, uma equipe de identificação de vítimas e conexão à base de dados internacional da Interpol.⁶

Os riscos da internet são muitos, em especial para a criança e o adolescente, que, em razão de sua personalidade estar em franco desenvolvimento, muitas vezes não consegue perceber os perigos e se comportar de forma a proteger-se.

Por tais motivos, os aliciadores encontram, neste terreno, uma possibilidade de saciar suas necessidades e envolver a vítima, seduzindo-a, fazendo com que acreditem que são confiáveis e protetores, embora queiram, na verdade, explorá-la. As práticas de pedofilia na internet se apresentam de várias formas; o acesso às páginas com material de exploração sexual de crianças e adolescentes são exemplos comuns desse tipo de ação criminosa; a produção, a publicação, a compra e a venda deste material, além do aliciamento das vítimas, a prática de sexo *on-line* interativo, dentre outros, também caracterizam o delito, sendo todos os casos permeados de violência infantojuvenil.

2.1 Riscos presentes no uso da *internet*

Por ser um espaço público, onde o acesso no mundo inteiro é praticamente irrestrito, a internet apresenta diversos riscos, especialmente no que se refere à criança e ao adolescente, destacando-se as seguintes categorias por serem as mais usuais no que se refere à captação de crianças e adolescentes com intenções sexuais:

1. *Grooming*: são atividades de persuasão praticadas por um agressor, normalmente adulto, em relação a uma criança ou a um adolescente, com a intenção de convencê-la a realizar atividades sexuais. Trata-se de uma espécie de aliciamento, de sedução para que o infante se sinta atraído e compelido a colaborar com as intenções do agressor.

Normalmente, o *grooming* é praticado por pessoas da mesma região da criança ou adolescente. Como a interação entre a vítima e o agressor é requisito essencial, ambos devem se comunicar no mesmo idioma, restringindo, assim, muitas vezes, a localização dos protagonistas. Não é raro, no entanto, que os agressores falem diversos idiomas, dificultando as investigações.

O *grooming* pode chegar à prática de encontros virtuais, com troca de imagens ou vídeos, favorecendo a ocorrência de estupro virtual, ou ainda, podendo propiciar encontros pessoais para a prática de relações sexuais ou outros atos libidinosos entre o agressor e a vítima.

⁶ ASSEMBLEIA GERAL DA INTERPOL – Resolução nº AG-2011-RES-08. Disponível em: <file:///E:/Users/kassiany/Downloads/AG-2011-RES-08.pdf>. Acesso em: 18 out.2017.

Para a prática do *grooming*, o autor muitas vezes assume identidade de outra pessoa, obtendo dados e fotos falsas, criando perfis sociais fictícios conhecidos por “*fakes*”, justamente para iludir as vítimas e dificultar sua identificação.

2. *Sexting*: caracteriza-se pelo envio de conteúdo sexual produzido pelo próprio indivíduo, sendo remetido para outras pessoas geralmente através de dispositivos móveis com acesso a *internet* como *smartphones*, *tablets*, *webcam*, computadores, *notebooks*. São conhecidos por “*nudes*”, que correspondem às imagens íntimas da vítima ou à atividade de natureza sexual. Muito utilizado por adolescentes que desavisados dos perigos da *internet* acreditam que as pessoas para quem enviam as imagens são de confiança e jamais divulgariam seu conteúdo. Infelizmente, essa espécie de exposição na *internet* é muito comum e causa danos irreparáveis às vítimas que, frequentemente, sofrem com a exposição indevida, chegando, nos casos mais graves, à situação extrema como a prática de suicídio quando não conseguem suportar emocionalmente as consequências desta espécie de exposição.

O *sexting*, em alguns casos, decorre do *grooming*, uma vez que depois de aliciar ciberneticamente a vítima, o agressor obtém dela as imagens de “*nudes*”. Essas imagens poderão dar ensejo ao *sexortion*, ou a extorsão propriamente dita, com a finalidade de exigir da vítima, ou de seus familiares, vantagens ilícitas. Os “*nudes*” normamente são transmitidos através de dispositivos ou aplicativos ponta a ponta, como o *WhatsApp*, onde as imagens são enviadas de uma pessoa para outra, de forma criptografada. Mas também podem ser compartilhadas em grupos ou outros aplicativos e até postadas em sites na internet.

3. *Sexortion*: é a extorsão, oportunidade em que o criminoso solicita favores sexuais ou vantagem econômica, em troca de não tornar público textos, imagens ou vídeos íntimos de suas vítimas. Nesta situação, muitas vezes, a vítima que protagonizou as mensagens ou imagens pode ser chantageada, como também seus familiares. Entretanto, ela é mais eficaz contra as crianças e os adolescentes por serem alvos frágeis em razão da sua condição especial de desenvolvimento. Sabe-se que os jovens, muitas vezes, para tentar esconder situações de *sexting* nas quais se envolveram, acabam cedendo às investidas de seus algozes. Essas vítimas, na maioria das vezes jovens, com vergonha e medo da repercussão social e familiar de suas fotos, sentindo-se responsáveis pelo envio delas ao seu algoz, acabam por sucumbir aos desejos deste.

Esse tipo de extorsão pode ocorrer de forma pouco sofisticada, mas, normalmente, os autores são pessoas organizadas que estruturam uma rede de atuação de forma a alcançar, com segurança, seus objetivos. A rede que pratica o

sextortion é composta pelo líder, recruta, agente e vítima. O líder é quem organiza a rede, o recruta é quem oferece ao agente ou chantagista um incentivo mensal dependendo da *performance* deste. O agente ou aliciador, assume identidades diferentes para atrair a vítima, aliciando-a em aplicativos ou *sites* sociais da *internet*. E, finalmente, a vítima, maioria jovens usuários de aplicativos e das redes sociais na internet que se envolvem com os aliciadores.⁷

4. O *Cyberbullying*, ou *bullying virtual*:⁸ o *bullying*⁹ é um comportamento agressivo e não desejado entre crianças, adolescentes e adultos, que se caracteriza pelo desequilíbrio do poder.¹⁰ Observe-se que aqui, por ser um ambiente cibernético, onde uma única ação pode repercutir mundialmente, não é exigida a reiteração das agressões para a configuração do *cyberbullying*. As crianças e os adolescentes que se expõem sexualmente na internet podem estar sujeitos ao *cyberbullying* tanto por parte dos pares, também crianças e adolescentes, como por parte de adultos, considerando que, na rede de *internet*, nem sempre está claro quem é criança, adolescente e adulto, haja vista a possibilidade de serem adotadas identidades falsas. O *cyberbullying* pode ocorrer pela discriminação, exclusão, ofensas, e desvalorização da vítima praticado por grupos na rede de computadores. Não raras vezes estas atitudes cibernéticas migram para a vida real, causando danos irreparáveis às vítimas. As consequências deste tipo de violência, tanto no mundo cibernético quanto no real, são graves. Há situações em que ocorre inclusive o incentivo a prática de suicídio. As crianças e os adolescentes, mais uma vez fragilizados pela situação, acabam sucumbindo aos desmandos de seus agressores.
5. *Malware*: são famílias de vírus que apagam ligações e mensagens, enviam por controle remoto mensagens a todas as pessoas de contato da vítima, capturam chamadas telefônicas, listas, nomes, números, imagens, gravam conversas, mensagens e vídeos, falsificam perfis, simulam problemas técnicos etc. Após a obtenção dos dados, os malfeitores usam as informações capturadas para extorquir as vítimas. A situação se agrava em razão

⁷ LAZARO, FERNANDES. Coordenador Forense Digital. Ferramentas e servicios del complejo mundial para La Innovacion – Complejo Mundial para La innovacion de INTERPOL. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires, Argentina, em 11 de junho de 2015.

⁸ SILVA, Ana Beatriz Barbosa. *Bullying: mentes perigosas nas escolas*. Rio de Janeiro: Objetiva, 2010.

⁹ BRASIL. Lei nº 13.185, 6 de novembro de 2015. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/13185.htm>. Acesso em: 11 jan. 2011. Acesso em 16/03/2019.

¹⁰ FANTE, Cleo; PEDRA, José Augusto. *Bullying escolar: perguntas & respostas*. Porto Alegre: Artmed, 2008. p. 37.

do aperfeiçoamento da tecnologia, pois o *malware* pode ser instalado em qualquer equipamento como computadores, *smartphones*, *smarttv* podendo obter as informações sem o conhecimento do usuário do equipamento.

Assim, textos, áudios e imagens podem ser capturados por estes dispositivos, sem que a vítima tenha conhecimento e, posteriormente, utilizados para extorsão contra elas e suas famílias.

Estudos sobre os perigos da internet realizados pela *Symantec* acerca do cibercrime (*Norton Cybercrime Report*) através de um relatório com diversas temáticas no mundo e no Brasil, em 2011,¹¹ nos trazem uma ideia sobre o comportamento das crianças e adolescentes no ambiente cibernético que causa muita preocupação para os atores que trabalham com a proteção infantojuvenil:

Alguns dos dados abaixo chamam atenção para esse tema:

- 71% dos adolescentes escondem de seus pais seu comportamento na *internet*.
- 46% dos jovens reconheceram ter acessado, de maneira acidental, a sites pornográficos na web.
- 32% admitem ter acessado sítios pornográficos de maneira intencional.
- 23% dos adolescentes utilizam computador não controlado pelos pais.
- 23% ocultam detalhes ou mentem sobre suas atividades na internet.
- 34% ocultam ou eliminam mensagens instantâneas em vídeos.
- 40% fecham ou minimizam o navegador quando os pais estão chegando.
- 87% dos pais cujos filhos tiveram experiências negativas na internet, também foram vítimas de crimes cibernéticos.
- 67% dos adolescentes limpam seu histórico do navegador (*browser history*) para que seus pais não tomem conhecimento de seus acessos.
- 64% dos pais não utilizam controle através de *software* que filtram os acessos.

Entretanto, um dos dados mais graves fornecidos pela Norton apontam no sentido de que um a cada dez adolescentes manifestaram ter encontrado na vida real alguém que haviam conhecido na internet. Isso evidencia o alto grau de vulnerabilidade a que estão expostas as crianças e adolescentes que acessam a rede internacional de computadores.

Essas informações são importantes para o desenvolvimento de medidas de prevenção eficazes na proteção de crianças e adolescentes. Nos dias de hoje, a ideia de que os programas ou filtros instalados pelos pais para bloquear esse tipo de acesso a sites adultos nos computadores não são mais suficientes.

¹¹ SYMATENC. Norton Cybercrime Report. 2011. Disponível em: <<http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf>>. Acesso: 16 mar. 2019.

Com o avanço da tecnologia, crianças e adolescentes utilizam equipamentos móveis como *smartphones* para se comunicarem e acessarem a internet de forma irrestrita e com pouca supervisão de um adulto. Com esses aparelhos, conseguem ficar *on-line* o tempo todo, em qualquer lugar, postando nas redes sociais, com frequência, dados capazes de indicar o local em que estão, através do “*check in*”, bem como o que estão fazendo, tornando-se, assim, alvos fáceis para os pedófilos.

Não raras vezes os pais, ao invés de protegerem seus filhos, os expõem nas redes sociais com fotografias e comentários, indicando a escola onde eles estudam, os horários de entrada e saída, sua casa, parques, praças, shoppings, clubes e outros lugares que costumam frequentar. Na grande maioria das vezes não se dão conta de que tornam público suas rotinas diárias e de seus filhos, bem como a condição sociofinanceira da família, colocando-se em situação de vulnerabilidade.

2.2 Processo de recrutamento da vítima

O processo de recrutamento da vítima na internet se dá especialmente pelo *grooming*. No entanto, ao escolher a vítima, o agressor leva em conta algumas características como: a baixa autoestima da vítima, sua situação de vulnerabilidade, alguma deficiência, e, especialmente a pouca ou inexistente supervisão de um adulto.

As estruturas familiares atuais favorecem que a criança e o adolescente, ainda muito jovens, circulem no mundo de adultos com pouco controle de um responsável que o alerte para os perigos da vida, inclusive digital. Desta forma ocorre uma exposição demasiada e indevida destas, que ainda se encontram em processo de formação. Em razão da exposição ficam suscetíveis ao *bullying* tanto na vida real quanto na internet, tornando-se ainda mais frágeis e vulneráveis.

A baixa autoestima pode ser causada por: questões pessoais, por alguma deficiência, pela intolerância às diferenças, pela rejeição e pelo *bullying*. Trata-se de terreno fértil para a atuação de exploradores sexuais. Vítimas assim vulneráveis possuem poucos amigos e se consideram pessoas não compreendidas, tanto pela família, como pela sociedade. Com esse histórico se tornam presas fáceis para os agressores.

Os exploradores sexuais infantojuvenis costumam frequentar locais onde a presença de crianças e adolescentes é constante, como parques, praças, *shoppings*, supermercados, igrejas, escolas, e especialmente, redes sociais da internet, sendo esta muito frequente e oportuna em razão do anonimato que proporciona.

Os agressores enganam, iludem as vítimas, manipulando-as de acordo com seus desejos e intenções, fazendo com que elas se enamorem por eles, seduzindo-as, mostrando-se inicialmente amigos e confidentes. Após conquistar a confiança das vítimas, e, às vezes, de seus familiares, começam os pedidos de contato com maior intimidade, quer virtualmente, quer pessoalmente. Para conquistar a vítima, podem alcançar alguma vantagem a ela, mas, em seguida, usam de violência e ameaça para manter suas conquistas e para que o segredo entre eles não seja revelado.

2.3 Prevenção

A prevenção continua sendo o melhor remédio para que crianças e adolescentes fiquem protegidos no ambiente cibernético. Conversar com a criança ou com o adolescente, tanto em casa quanto nas escolas, sobre diversos temas relacionados com sexo e internet é algo, hoje, obrigatório, assim como ensiná-las a se protegerem de situações que envolvam exploração sexual e outros crimes cibernéticos.

Entre diálogos e orientações às crianças e aos adolescentes e também a seus responsáveis destaca-se:

1. Evitar postagem de imagens das crianças e adolescentes nuas ou em poses sensuais em redes sociais.
2. Evitar postar imagens de crianças e adolescentes com uniformes da escola, ou em imagem que possa identificar a escola que frequentam.
3. Evitar postar imagens onde possa ser identificada a residência da criança ou do adolescente, bem como mostrar os bens que possuem.
4. Evitar postar imagens que identifiquem a rotina da criança ou adolescente, os lugares que normalmente frequenta ou ainda fazer “*check in*” em todos os locais que comparecer.
5. Divulgar uma cultura de paz e respeito na família e a maior participação dos pais na vida dos filhos.
6. Esclarecer as crianças, aos adolescentes, aos responsáveis e aos professores sobre o tema e o conceito de cidadania, inclusive digital.
7. Investir em educação socioemocional, apoiando as crianças e os adolescentes à aprenderem a expressar suas emoções e sentimentos sem a necessidade de agressividade, estimulando a solução pacífica de conflitos.

3 Críticas ao Estatuto da Criança e do Adolescente

A Legislação Brasileira ao longo dos anos evoluiu no tocante ao estabelecimento de regras para o uso da internet, criminalizando condutas que possam violar os direitos de crianças e adolescentes.

O Estatuto da Criança e do Adolescente prevê a criminalização de condutas praticadas pela internet em desrespeito aos direitos das crianças e adolescentes, a partir do artigo 241:

Art. 241: Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cenas de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.

Art. 241 – A: Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfico envolvendo criança ou adolescente:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§ 1º Nas mesmas penas incorrem quem:

I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o *caput* deste artigo;

II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o *caput* deste artigo.

§ 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o *caput* deste artigo.

Art. 241 – B: Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cenas de sexo explícito ou pornografia envolvendo criança ou adolescente:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§ 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o *caput* deste artigo.

§ 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 341 – A e 241 – C desta lei, quando a comunicação for feita por:

I – agente público no exercício de suas funções.

II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;

III- representante legal e funcionário responsável de provedor de acesso ou serviço prestado por meio de rede de computadores até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.

§ 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.

Observe-se que no *caput* do artigo 241 – B, os verbos nucleares são adquirir, possuir ou armazenar. Assim, à primeira vista, parece que o legislador não contemplou o ato de acessar páginas com material de exploração sexual infantojuvenil. Pode-se pensar, outrossim, que houve um equívoco que deixa descobertos de proteção os casos em que há o acesso a este tipo de sites. Entretanto, toda vez que um site com conteúdo de exploração sexual infantojuvenil é acessado, este fica registrado no aparelho que o acessou.

Art. 241 – C: Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação virtual:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único: Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do *caput* deste artigo.

Art. 241 – D: Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso.

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único: Nas mesmas penas incorre quem:

I – facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso.

II – pratica as condutas descritas no *caput* deste artigo com o fim de induzir criança e se exibir de forma pornográfica ou sexualmente explícita.

Ao analisar o artigo 241 – D, verifica-se que o legislador contemplou o “*grooming*” no “*caput*” do aludido artigo, mas entendeu em proteger apenas as crianças, afastando da proteção legal o “*grooming*” praticado contra adolescentes. Repete em ambos os incisos do parágrafo único a mesma posição. Esta posição fragiliza a proteção de adolescente no sistema legislativo pátrio. Neste sentido também é a posição de Murillo José Digiácomo e Ildeara de Amorim Digiácomo, ao comentar o equívoco legislativo no livro *Estatuto da Criança e do Adolescente Anotado e Interpretado*.¹²

O inciso II, do parágrafo único, indica a prática de divulgação de “*nudes*” quando a criança é induzida a enviar, ao agressor, imagens pornográficas suas, silenciando a proteção quanto ao adolescente.

Tal linha legislativa não parece adequada, considerando que a lei penal considera estupro de vulnerável quando o ato é praticado contra adolescente

¹² DIGIÁCOMO, Murillo José. *1969 – Estatuto da criança e do adolescente anotado e interpretado* / Murillo José Digiácomo e Ildeara Amorim Digiácomo. Curitiba. Ministério Público do Estado do Paraná. Centro de Apoio Operacional das Promotorias da Criança e do Adolescente, 2017. 7. ed. p. 385.

menor de 14 anos de idade,¹³ lembrando que pelo conceito legal a adolescência compreende o período etário dos 12 aos 18 anos de idade, conforme artigo 2º, da Lei nº 8.069/90, Estatuto da Criança e do Adolescente.¹⁴

Como se sabe, o Brasil é signatário da Convenção das Nações Unidas para a proteção das crianças e dos adolescentes. Em razão disso a Constituição Federal de 1988, conhecida por Constituição Cidadã, no artigo 227, contempla o princípio constitucional da Prioridade Absoluta, que posteriormente foi adotado pelo Estatuto da Criança e do Adolescente no artigo 4º e seu parágrafo único, o qual prevê que a garantia de prioridade compreende: primazia de receber proteção e socorro em quaisquer circunstâncias, precedência de atendimento nos serviços públicos ou de relevância pública, preferência na formulação e na execução das políticas sociais públicas, destinação privilegiada de recursos públicos nas áreas relacionadas com a proteção à infância e à juventude.

Estes marcos legais são importantes, pois nos trazem a noção exata de que há um interesse internacional na proteção de crianças e adolescentes e que o Brasil, através de sua legislação constitucional e infraconstitucional, se compromete a garantir este direito.

Pelo Estatuto da Criança e do Adolescente, segundo o artigo 2º, considera-se criança a pessoa até 12 anos de idade incompletos, e adolescente aquela entre 12 a 18 anos de idade. Este diploma legal também adota, no artigo 3º, o princípio da proteção integral, onde todas as crianças e todos os adolescentes gozam dos direitos fundamentais inerentes à pessoa humana, assegurando-lhes por lei ou por outros meios, todas as oportunidades e facilidades, a fim de lhes facultar o desenvolvimento físico, mental, moral, espiritual e social, em condições de liberdade e de dignidade. Na mesma esteira, o artigo 5º desta lei, estabelece que nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punindo na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais.

Assim, qualquer criança ou adolescente deveria estar protegido pelo artigo 241 – D em sintonia com os demais dispositivos do próprio Estatuto da Criança e do Adolescente, do Código Penal, Constituição Federal e normas internacionais.

¹³ Art. 217 – A: Ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos: Pena – reclusão, de 8 (oito) a 15 (quinze) anos § 1º Incorre na mesma pena quem pratica as ações descritas no *caput* com alguém que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência. BRASIL. *Código Penal (1940)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 16 mar. 2019.

¹⁴ BRASIL. Lei nº 8.069, de 13 de julho de 1990. *Estatuto da Criança e do Adolescente*. Disponível em: <www.planalto.gov.br/Ccivil_03/leis/L8069.htm>. Acesso em: 16 mar. 2019.

Observe-se que este tipo de crime atinge principalmente a faixa etária entre 10 a 14 anos de idade.

Art. 241 – E: Para efeito dos crimes previstos nesta Lei, a expressão “cena de sexo explícito ou pornográfica” compreende qualquer situação que envolva criança ou adolescente em atividades sexuais, explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

Este artigo define a expressão “cenas de sexo explícito ou pornográfica”, estabelecendo que as publicações devam ter fins primordialmente sexuais. Segundo Murillo José Digiácomo e Ildeara de Amorim Digiácomo, ao comentar este artigo no livro *Estatuto da Criança e do Adolescente Anotado e Interpretado*, referem que o legislador quis evitar possíveis dúvidas quanto ao alcance da norma proibitiva, que deve ser o mais abrangente possível, em observância aos arts. 1º, 5º, 6º e 100, parágrafo único, inciso II, do ECA.¹⁵

4 Produção da prova

Para judicializar as ações, tanto na área cível quanto criminal, a constituição da prova é essencial.

A coleta da prova passa, principalmente, pela perícia técnica dos equipamentos apreendidos. Hoje, existem equipamentos próprios para efetuar essas perícias que fornecem, inclusive, certificação sobre a extração do conteúdo apreendido.

A vigilância do agressor traz um potencial interessante na obtenção do local onde a prova pode ser encontrada. Assim, informações a respeito dos lugares que o agressor frequenta, o carro que possui, tipo de acessórios que utiliza como mala e bolsa, por exemplo, com quem mantém contato e sua rotina, podem ser úteis durante as investigações. A abordagem do agressor deve ser cuidadosa, considerando que há alto índice de suicídio deste, quando descoberto.

A entrevista com o agressor pode auxiliar na obtenção de informações sobre senhas de acesso aos equipamentos, às redes sociais, aos arquivos, inclusive à *nuvem*, além de codinomes, frequência a *sites* acessados, para a localização do material relacionado à exploração sexual infantojuvenil. A apreensão de equipamentos como: *pendrives*, CDs/DVDs e outros dispositivos, assim como a identificação do local de armazenamento de dados na *nuvem* são informações importantes, porque podem conter elementos fundamentais para a materialização de

¹⁵ DIGIÁCOMO, Murillo José, 1969-Estatuto da criança e do adolescente anotado e interpretado / Murillo José Digiácomo e Ildeara Amorim Digiácomo. Curitiba. Ministério Público do Estado do Paraná. Centro de Apoio Operacional das Promotorias da Criança e do Adolescente, 2017. 7. ed. p. 386.

delitos. Os procedimentos investigatórios passam por rastreamento dos IPs, nomes de usuários, *e-mails*, redes sociais, e, para tanto, existem programas gratuitos que podem auxiliar na investigação. Também devem ser observadas todas as redes sociais da vítima e do agressor, avaliando-se os grupos de amigos e armazenamento na nuvem.

Quando forem encontradas imagens de crianças e de adolescentes em situação de exploração sexual infantil, é importante verificar se as vítimas já foram identificadas. Existem programas específicos como por exemplo o EXIF,¹⁶ que auxiliam nesta tarefa. Também é necessário verificar se as imagens foram alteradas eletronicamente, e isso pode ser obtido pelo número de *pixels* de cada imagem. Durante a investigação da imagem, é importante avaliá-la, procurando detalhes que possam identificar tanto a vítima como o local fotografado ou filmado, pois as informações podem auxiliar na localização da vítima.

A oitiva da criança pode ser importante para a identificação do agressor e entendimento de sua forma de atuação.

O material apreendido, muitas vezes, vai auxiliar a determinar a competência para propositura das ações, pois, é através dele, que informações podem ser obtidas sobre a internacionalidade das ações ou não, sobre as vítimas envolvidas e as responsabilidades das operadoras ou empresas responsáveis pelo *sites* que hospedam as imagens de exploração sexual infantojuvenil.

O objetivo principal deve ser sempre o de cessar a violência sexual contra a criança ou o adolescente, buscando a localização e a proteção da vítima.

5 Escuta especializada e depoimento especial da criança e do adolescente, em conformidade com a Lei Federal nº 13.431/17

A entrevista de crianças e de adolescentes, através da escuta especializada e do depoimento especial¹⁷ é um tema delicado. Se, por um lado as crianças e

¹⁶ MACNAMARA, Maximiliano. Analista de la Subdirección de trata de Personas y Explotacion Infantil de INTERPOL. Las herramientas y servicios de INTERPOL para combatir la explotacion sexual infantil em línea. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires, Argentina, em 11 de junho de 2015.

¹⁷ Art. 7º: Escuta especializada é o procedimento de entrevista sobre situação de violência com criança ou adolescente perante órgão da rede de proteção, limitado o relato estritamente ao necessário para o cumprimento de sua finalidade e art. 8º: Depoimento especial é o procedimento de oitiva de criança ou adolescente vítima ou testemunha de violência perante autoridade policial ou judiciária. BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 18 out. 2017. Art. 12 da Convenção Internacional dos Direitos da Criança, adotado pela Assembleia das Nações Unidas, em 1989. Disponível em: <https://www.unicef.org/brazil/pt/resources_10127.htm>. Acesso em: 18 out. 2017.

os adolescentes têm o direito de serem ouvidos,¹⁸ regra preconizada por normas nacionais e internacionais, por outro, existe a necessidade de proteção destas vítimas, em razão das consequências emocionais ocasionadas pela revitimização de procedimentos de entrevista inadequados e consecutivos, capazes de influenciar no relato de crianças e adolescentes, retirando destes sua autenticidade e credibilidade.

Diferente da vida real, onde a prova da violência sexual é difícil de ser produzida diante da inexistência de testemunhas, sobretudo quando não deixa vestígios, no mundo cibernético existe a possibilidade de obtenção de evidências através de investigações específicas, que podem dispensar a entrevista com a criança e o adolescente. Partindo desta premissa, e do disposto pela legislação pátria, a entrevista com a criança, no sistema de proteção, de segurança e de justiça deve ter como fundamento ouvir a vítima apenas uma vez ou o mínimo de vezes possível, observando a necessidade. Entretanto, muitas vezes é imperioso que a criança ou o adolescente seja ouvido, e, nesse caso, esta oitiva deverá ser feita em conformidade com a Lei Federal nº 13.431/2017, utilizando-se um protocolo de entrevista investigativa,¹⁹ uma vez que as técnicas utilizadas para coletar um depoimento constituem um dos fatores de maior influência na qualidade de um relato.²⁰

Embora pela legislação nacional, a aplicação de protocolo só seja exigível para o Depoimento Especial, aquele que ocorre perante a autoridade policial e judicial, é prudente que na escuta especializada o entrevistador tenha os mesmos cuidados. Não faz sentido proceder ao Depoimento Especial com toda a cautela, ficando a escuta especializada, primeiro momento em que a criança é ouvida, desprotegida e a mercê de profissionais não qualificados.

A entrevista investigativa é regida por protocolo. Os protocolos mais conhecidos e validados internacionalmente são a entrevista investigativa (estruturada ou semiestruturada) e o Nichd (*National Institute of Child Health and Human Development*). Todos os protocolos possuem similitude.

¹⁸ Art. 5º: A aplicação desta Lei, sem prejuízo dos princípios estabelecidos nas demais normas nacionais e internacionais de proteção dos direitos da criança e do adolescente, terá como base, entre outros, os direitos e garantias fundamentais da criança e do adolescente a: VI – ser ouvido e expressar seus desejos e opiniões, assim como permanecer em silêncio. BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 18 out. 2017.

¹⁹ Art. 11: O depoimento especial reger-se-á por protocolos e, sempre que possível, será realizado uma única vez, em sede de produção antecipada de prova judicial, garantida a ampla defesa do investigado. BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 12 mar. 2019.

²⁰ WELTER, Carmen Lisboa W., LOURENÇO, Ana Paula Schmidt, ULLRICH, Larissa Brasil, STEIN, Lilian Milnitsky, PINHO, Maria Salomé. *Considerações sobre o depoimento de criança/adolescente vítima de violência sexual*. Ministério Público do Rio Grande do Sul. Disponível em: <<https://www.mprs.mp.br/media/areas/infancia/arquivos/revistamulti1.pdf>>. Acesso em: 16 mar. 2019.

De regra, os protocolos possuem etapas que asseguram que a criança ou o adolescente não fique exposto a mais violência²¹ durante o fornecimento do relato. Independente de ser a escuta especializada ou o depoimento especial, algumas noções básicas devem reger a coleta do testemunho, para que as evidências obtidas tenham credibilidade e a criança ou adolescente não seja revitimizada.

Um dos requisitos é o ambiente onde a criança ou o adolescente será entrevistado, o qual deve ser confortável ou ao menos que inspire segurança, sem a presença do suposto agressor e pessoas estranhas, além da técnica que conduzirá a entrevista. Recomenda-se que na sala não existam elementos que possam distraí o entrevistado, de forma que facilite sua concentração para a produção de um relato confiável.²² A criança ou testemunha de violência como prevê a Lei 13.431/2017,²³ tem o direito de se manifestar em todos os feitos administrativos e judiciais que lhe digam respeito, mas também tem o direito ao silêncio. É mister que esse direito seja respeitado.

Para a entrevista propriamente dita, devem ser aplicados protocolos validados internacionalmente baseados em princípios técnicos das boas práticas de entrevista investigativa fundamentadas na literatura científica. A maioria dos protocolos seguem alguns passos que são semelhantes.

²¹ Art. 12: O depoimento especial será colhido conforme o seguinte procedimento:

I – os profissionais especializados esclarecerão a criança ou o adolescente sobre a tomada do depoimento especial, informando-lhe os seus direitos e os procedimentos a serem adotados e planejando sua participação, sendo vedada a leitura da denúncia ou de outras peças processuais;

II – é assegurada à criança ou ao adolescente a livre narrativa sobre a situação de violência, podendo o profissional especializado intervir quando necessário, utilizando técnicas que permitam a elucidação dos fatos;

III – no curso do processo judicial, o depoimento especial será transmitido em tempo real para a sala de audiência, preservado o sigilo;

IV – findo o procedimento previsto no inciso II deste artigo, o juiz, após consultar o Ministério Público, o defensor e os assistentes técnicos, avaliará a pertinência de perguntas complementares, organizadas em bloco;

V – o profissional especializado poderá adaptar as perguntas à linguagem de melhor compreensão da criança ou do adolescente;

VI – o depoimento especial será gravado em áudio e vídeo.

BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 16 mar 2019.

²² Art. 10: A escuta especializada e o depoimento especial serão realizados em local apropriado e acolhedor, com infraestrutura e espaço físico que garantam a privacidade da criança ou do adolescente vítima ou testemunha de violência. BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 16 mar. 2019.

²³ BRASIL. Lei nº 13.431, de 4 de abril de 2017. Disponível em: <www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 24 mar. 2018.

O primeiro momento da entrevista é chamado de *rapport*, que se caracteriza por uma breve conversa sobre temas diversos do objeto da entrevista, abordando tópicos de interesse da vítima, visando a testar a memória e criar uma relação de confiança entre o entrevistador e entrevistado.

Informar a vítima, criança ou adolescente, sobre o motivo pelo qual está sendo ouvida e que tem o direito de não querer falar. Mas se a vítima desejar contar o ocorrido deverá ser orientada a dizer a verdade, pois é ela quem detém o conhecimento. Deverá, ainda, ser esclarecida de que caso não se lembre de algo poderá informar que não recorda dos fatos, e isso não invalidará as demais declarações. É o momento onde é oferecido instruções para o relato.

A etapa seguinte é a do relato livre, ou seja, a vítima deverá noticiar os fatos de forma livre, sem que haja interrupção por parte do examinador. Para a recuperação da memória, pode-se auxiliar a reconstituição mental do local onde os fatos ocorreram, estimulando a memória para que se recorde de cheiros, clima, etc., fornecendo comandos que acessem a memória de recordação livre. Nesta etapa, caso a vítima tenha dificuldade em falar, o examinador poderá estimular a vítima a fazê-lo, mas evitará interferir no relato ou fazer perguntas específicas.

Recuperação focada, momento em que a vítima é questionada através de perguntas abertas com ênfase nas seguintes questões, caso não tenham sido esclarecidas anteriormente:

- Quais equipamentos foram utilizados, se havia controle dos responsáveis, quem estava junto quando houve o acesso e/ou contato com o agressor.
- Onde e como o acesso era feito, e quais sites, aplicativos, redes sociais, etc. eram utilizados.
- Horário dos acessos.
- Nomes/apelidos que utilizava para falar com o agressor.
- Nomes/apelidos usados pelo agressor.
- Quais suas senhas e se foram fornecidas ao agressor, assim como se foram fornecidas informações pessoais ao agressor.
- Conteúdo das conversas.
- Se houve troca de imagens como fotos, desenhos ou vídeos, suas ou de seu agressor.
- Se recebeu fotos, desenhos ou vídeos envolvendo outras crianças.
- Esclarecer se sofreu ameaças, intimidação para fornecer informações ou para praticar algum ato, relatando as circunstâncias.
- Se houve encontro pessoal com o agressor, descrever o local, o agressor e terceiros que por ventura também estavam no local, sejam vítimas ou agressores.
- Descrição das pessoas com que manteve contato *on-line*, caso seja possível.
- Se alguém tomou conhecimento do ocorrido, identificando a pessoa.

Para esclarecer dúvidas ou contradições, deve-se conduzir a entrevista com a maior neutralidade possível, sem indução ou sugestões, nem valoração da conduta da vítima entrevistada.

Ao término, o entrevistador deve deixar a criança confortável, voltando a falar sobre assuntos neutros e deixando contato para, caso a criança recorde de algo, possa retornar para relatar ao examinador.

Verificar se a criança está bem ou não, e encaminhá-la para a rede de proteção, uma vez que a entrevista faz com que a criança reviva a situação de violência.

Especialmente nos crimes cibernéticos, existe a possibilidade da criança e do adolescente não perceberem a violência como tal. A não percepção da situação de violência pode ser benéfica dando origem a um relato menos contaminado. Tal circunstância auxilia o investigador forense, já que a vítima fica mais a vontade para fazer os relatos. Quanto mais informações forem prestadas, mais elevada será a credibilidade do testemunho.

Não é demais lembrar ao examinador que se abstenha de fazer qualquer juízo de valor, para que a vítima não se sinta culpada.

6 Marco Civil da Internet – Lei nº 12.965 de 23 de abril de 2014

Essa lei tem por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determinar as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. Estabelece regras para o funcionamento de serviços de Internet, como equipamentos de procura e redes sociais, e tenta sanar as divergências entre as decisões de tribunais brasileiros, em relação à responsabilidade em casos de armazenamento e circulação de conteúdo indevido, gerados por usuários em serviços como *Google*, *Facebook*, etc.

A Lei do Marco Civil da Internet²⁴ auxilia na manutenção da prova para atuação criminal e cível e introduz uma série de conceitos e termos técnicos para a garantia de direitos dos usuários e estabelece diretrizes para atuação do poder público. Estabelece, ainda, princípios relativos à privacidade e à proteção de dados pessoais, como também regras de retenção de dados e registros eletrônicos por parte de provedores de serviços de internet.

²⁴ BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 16 mar. 2019.

Essa lei preconiza a preservação, por seis meses, dos registros de acesso a aplicativos de internet.²⁵ Já os registros de conexão devem ser preservados por um ano, podendo o prazo ser superior a pedido do Ministério Público, Polícia ou autoridade administrativa.²⁶

A lei introduz regras para a requisição de dados de entidades públicas e privadas, estabelecendo que as informações dos provedores somente poderão ser obtidas por ordem judicial. Infelizmente esta regra prejudica as investigações dos delitos cibernéticos, especialmente no que tange a proteção de crianças e de adolescentes, contrariando o disposto no Estatuto da Criança e do Ado-

²⁵ Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. § 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado. § 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no *caput*, observado o disposto nos §§ 3º e 4º do art. 13. § 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. BRASIL. Lei nº 12.965 de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em 16 mar. 2019.

²⁶ Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. § 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros. § 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput*. § 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no *caput*. § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º. § 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo. § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência. BRASIL. Lei nº 12.965 de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

lescente, que autoriza a requisição, pelo Ministério Público, de informações tanto de órgãos públicos como privados conforme disposto no artigo 201, do Estatuto da Criança e do Adolescente.²⁷

A lei do marco civil estabelece o tratamento de dados pessoais, como necessidade de consentimento expresso, claro e informado do usuário e diversas restrições para o seu gerenciamento e envio para terceiros.

O artigo 11, § 2º da Lei do Marco Civil da Internet²⁸ estabelece que provedores com representação no Brasil ou que prestes serviços neste país devem cumprir a legislação nacional.

O Marco Civil da Internet institui as responsabilidades dos provedores, e o artigo 18²⁹ estabelece que o provedor não responde civilmente por danos decorrentes de conteúdo gerado por terceiros. Contudo, responderá, caso não adote as medidas necessárias após ordem judicial, conforme artigo 19 do mesmo diploma legal.³⁰ O artigo 21³¹ desta lei decreta que o provedor deve retirar material contendo nudez ou ato sexual, após cientificado, mediante simples notificação, sob pena de responsabilidade.

Na verdade, embora a lei seja clara quanto à retirada de material de pornografia infantil da internet, muitas vezes a medida fica difícil de ser executada, uma vez que os sites podem estar hospedados em países que não possuem acordos diplomáticos de reciprocidade com o Brasil. Uma vez postado na internet, mesmo com ações e decisões judiciais de retirada do material e/ou desindexação do conteúdo, nem sempre a proteção é obtida de forma plena, com a retirada de todas as imagens. Assim, a prevenção ainda é a melhor medida que se apresenta.

7 Considerações finais

Considerando a natureza e as características da internet, especialmente a publicidade e a dificuldade de retirar os conteúdos postados, o investimento na prevenção ainda é a medida protetiva mais eficaz.

²⁷ BRASIL. Lei nº 8.069, de 13 de julho de 1990. *Estatuto da Criança e do Adolescente*. Disponível em: <www.planalto.gov.br/Ccivil_03/leis/L8069.htm>. Acesso em: 16 mar. 2019.

²⁸ BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

²⁹ BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

³⁰ BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

³¹ BRASIL. Lei nº 12.965, de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

Trabalhar na prevenção, especialmente junto às escolas, esclarecendo às crianças e aos adolescentes sobre o uso seguro da internet, bem como alertando os genitores e profissionais da área da educação sobre como abordar o tema com seus filhos e alunos buscando sempre a proteção no campo cibernético, é uma alternativa, que gera um bom resultado.

Articular buscando a cooperação entre as instituições públicas, do âmbito estadual e federal, com atribuições para investigar, processar e julgar os casos envolvendo crimes cibernéticos e suas consequências na área cível e de proteção às crianças e aos adolescentes, com a criação de fluxos e protocolos de atuação.

Qualificar os operadores do direito para atuarem com maior conhecimento nesta matéria criando estruturas próprias ou compartilhando as já existentes.

Atuar buscando a cooperação entre instituições públicas e privadas no combate a estas questões.

Revisar a legislação existente para promover a proteção efetiva das crianças e dos adolescentes e punição de seus agressores.

E por fim, não descuidar de encaminhar as crianças e adolescentes vítimas e testemunhas das violações de direitos para as instituições que fazem parte do SGDCA (Sistema de Garantias de Direitos da Criança e do Adolescente) mais especificamente, para o sistema de proteção a fim de que procedam nos atendimentos adequados, em saúde, educação e assistência social, para tentar minimizar as consequências das violações, devolvendo a criança ou o adolescente e sua família, a dignidade.

Referência

ASSEMBLEIA DAS NAÇÕES UNIDAS. *Convenção Internacional dos Direitos da Criança (1989)*. Disponível em: <https://www.unicef.org/brazil/pt/resources_10127.htm>. Acesso em: 18 out. 2017.

ASSEMBLEIA GERAL DA INTERPOL. *Resolução nº AG-2011-RES-08*. Disponível em: <<file:///E:/Users/kassiany/Downloads/AG-2011-RES-08.pdf>>. Acesso em: 18 out. 2017.

BRASIL. *Código Penal (1940)*. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/De12848compilado.htm>. Acesso em: 16 mar. 2019.

BRASIL. *Constituição Federal (1988)*. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 16 mar. 2019.

BRASIL. Lei nº 8.069 de 13 de julho de 1990. Disponível em: <http://www.planalto.gov.br/civil_03/leis/L8069.htm>. Acesso em: 16 mar. 2019.

BRASIL. Lei nº 12.965 de 23 de abril de 2014. *Lei do Marco Civil da Internet*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm>. Acesso em: 16 mar. 2019.

BRASIL. Lei nº 13.185, 6 de novembro de 2015. *Lei do Bullying*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/113185.htm>. Acesso em: 11 jan. 2011. Acesso em: 16 mar. 2019.

BRASIL. Lei nº 13.431 de 4 de abril de 2017. *Lei da Escuta Protegida*. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13431.htm>. Acesso em: 16 mar. 2019.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. *Roteiro de atuação: crimes cibernéticos* / 2. Câmara de coordenação e revisão. 3. es. rev. e ampl. Brasília: MPF, 2016.

CECI, S. J., & Bruck, M. (1995). *Jeopardy in the courtroom: A scientific analysis of children's testimony*. Washington: American Psychological Association, Washington, DC, US.

DIGIÁCOMO, Murillo José. *1969 – Estatuto da criança e do adolescente anotado e interpretado* / Murillo José Digiácomo e Ildeara Amorim Digiácomo.- Curitiba. Ministério Público do Estado do Paraná. Centro de Apoio Operacional das Promotorias da Criança e do Adolescente, 2017. 7. ed.

FANTE, Cleo; PEDRA, José Augusto. *Bullying escolar: perguntas & respostas*. Porto Alegre: Artmed, 2008. p. 37.

LAMB, M. E.; Hershkowitz, I.; Orbach, Y., & Espin, P. W. (2011). *Tell me what happened, Structured Investigative Interviews of Child Victims and Witnesses*, Wiley series in the Psychology of Crime, Policing and law, Wiley-Blackwell, England

LAZARO, FERNANDES. Coordenador Forense Digital. *Ferramentas e servicios del complejo mundial para La Innovacion – Complejo Mundial para La innovacion de INTERPOL*. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires-Argentina, em 11 de junho de 2015.

MACNAMARA, Maximiliano. Analista de la Subdirección de trata de Personas y Explotacion Infantil de INTERPOL. *Las herramientas y servicios de INTERPOL para combatir la explotacion sexual infantil em línea*. 2015. Palestra realizada na sede da INTERPOL, em Buenos Aires, Argentina, em 11 de junho de 2015.

Poole, D. A., & Lamb, M. E. (2009). *Investigative Interviews of Children, Guide for Helping Professional*, American Psychological Association, Washington, DC, US.

SILVA, Ana Beatriz Barbosa. *Bullying: mentes perigosas nas escolas*. Rio de Janeiro: Objetiva, 2010.

SYMATENC. *Norton Cybercrime Report 2011*. Disponível em: <http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrime/assets/downloads/en-us/NCR-DataSheet.pdf>. Acesso: 18 out. 2017.

WELTER, Carmen Lisboa W., LOURENÇO, Ana Paula Schmidt, ULLRICH, Larissa Brasil, STEIN, Lilian Milnitsky, PINHO, Maria Salomé. *Considerações sobre o depoimento de criança/ adolescente vítima de violência sexual*. Ministério Público do Rio Grande do Sul. Disponível em: <<https://www.mprs.mp.br/media/areas/infancia/arquivos/revistamulti1.pdf>>. Acesso em: 16 mar. 2019.