FACULDADE DE DIREITO DE CACHOEIRO DE ITAPEMIRIM - FDCI
CURSO DE GRADUAÇÃO EM DIREITO

FLÁVIA TANURE DA SILVA

CRIMES CIBERNÉTICOS

CACHOEIRO DE ITAPEMIRIM- ES
2017

FLÁVIA TANURE DA SILVA

CRIMES CIBERNÉTICOS

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito de Cachoeiro de Itapemirim - FDCI como requisito parcial para obtenção do grau de bacharel em Direito.
Orientador: Eduardo Pinheiro Monteiro

CACHOEIRO DE ITAPEMIRIM-ES
2017

FLÁVIA TANURE DA SILVA

CRIMES CIBERNÉTICOS

Aprovado em_____ de _____ de 2017

BANCA EXAMINADORA

_____

Prof. Orientador
Faculdade de Direito de Cachoeiro de Itapemirim – ES

_____

Prof. Examinador
Instituição de Ensino

_____

Prof. Examinador
Instituição de Ensino

AGRADECIMENTOS

Agradeço a Deus pela força, ânimo e saúde para superar e enfrentar todas barreiras, dificuldades e adversidades

Agradeço aos meus amigos por terem me proporcionado momentos felizes mesmo eu estando em um momento difícil na vida, sou muito grata por não terem deixado eu desistir no meio do caminho e estiveram nos momentos fáceis e difíceis e me mostraram que quando a pedras no caminho devemos recolhe-las e delas fazer um castelo.

Ao meu orientador investigador Eduardo Pinheiro Monteiro, pelo suporte e ajuda, no pouco tempo que lhe coube, pelas suas correções e incentivos para continuar.

Aos professores da instituição que ampliaram minha visão do mundo e ensinaram a questionar as divergências do mundo.

E a todos que direta e indiretamente fizeram parte da minha formação, o meu muito obrigado.

“Ando devagar porque já tive pressa e levo esse sorriso porque já chorei demais hoje me sinto mais forte mais feliz, quem sabe só levo a certeza de que muito pouco sei ou nada sei conhecer as manhas e as manhãs o sabor das massas e das maçãs é preciso amor pra poder pulsar é preciso paz pra poder sorrir é preciso a chuva para florir penso que cumprir a vida seja simplesmente compreender a marcha e ir tocando em frente”. (Almir Sater, Renato Texeira).

RESUMO

A presente monografia tem como objetivo discorrer sobre os aspectos da criminalidade com o auxílio da Internet, tendo em vista o seu aumento alarmante, alavancados pela massificação da Internet, a falsa impressão do anonimato e a comodidade que a grande rede oferece. Dessa forma à Internet trouxe para a sociedade novos criminosos, que precisam de regulamentação. Embora alguns crimes praticados no ambiente digital já se encontrem tipificados em nosso Código Penal, ainda é preciso criar condições técnicas e legais para a sua aplicabilidade. Na esteira desta evolução tecnológica, novas questões surgem, demandando respostas do operador do Direito, em face da velocidade das inovações que a tecnologia nos proporciona e os crimes que junto dela vão surgindo. Aos poucos o Direito brasileiro foi acompanhando a evolução tecnológica e nos tempos atuais já temos uma Internet que garanta o mínimo de segurança jurídica para que seja possível utilizá-la em sua plenitude.

Palavra-chave: Internet, ciberataque, crimes virtuais.

ABSTRACTY

This monograph aims to discuss the aspects of crime with the aid of the Internet, in view of its alarming increase, leveraged by the massification of the Internet, the false impression of anonymity and the convenience that the great network offers. In this way the Internet has brought to society new criminals, who need regulation. Although some crimes committed in the digital environment are already typified in our Penal Code, it is still necessary to create technical and legal conditions for their applicability. In the wake of this technological evolution, new questions arise, demanding answers from the operator of the Law, given the speed of the innovations that technology provides us and the crimes that come with it. Gradually the Brazilian law was following the technological evolution and in the present times we already have an Internet that guarantees the minimum of legal security so that it can be used in its fullness.

Keyword: Internet, cyberattack, virtuals crimes.

SUMÁRIO

1 INTRODUÇÃO

O presente trabalho tem como objetivo estudar os crimes que são praticados com o auxílio da internet.

Nos dias atuais, a Internet se tornou indispensável para grande parte da população mundial, nessa rede é possível pesquisar, estudar, fazer compras, namorar, trabalhar e uma infinidade de outras ações do dia a dia. Mas infelizmente, alguns criminosos têm utilizado esse avanço para realizar práticas delituosas com o intuito de obter para si, vantagem indevida em detrimento de outros internautas.

A cada segundo, milhões de computadores interligam-se por meio das linhas telefônicas no mundo inteiro, fazendo circular bilhões e bilhões de informações que se traduzem em movimentação financeira, intercâmbio cultural e inter-relacionamento pessoal entre pessoas e instituições de todas as partes do mundo e das mais variadas culturas.

A “febre” que surgiu mundialmente deve-se ao incrível mundo de informações, curiosidades e entretenimento que o usuário tem acesso nos mais variados e inusitados pontos do planeta. Com isto têm-se verificado uma miscigenação de culturas, dados e descobertas numa velocidade espantosa. A rede passou a ocupar um espaço muito importante na sociedade, demonstrando que é impossível ficar sem esse meio de comunicação. O uso da Internet se faz necessário em todos os segmentos econômicos e sociais, bem como na ciência do Direito.

Desde 1999, a imprensa em geral publica matérias noticiando casos de furto de dados, pedofilia, pornografias entre outros crimes.

Controlar a Internet deixou de ser uma preocupação social e passou a ser uma necessidade mundial, e é no Direito e na Justiça que podemos encontrar senão a perfeita, mas a sua melhor forma de controle.

2 HISTÓRIA DA EVOLUÇÃO DA INTERNET

A Internet, surgiu em plena guerra fria. Foi criada com objetivos militares. Servia para manter as comunicações norte-americanas, em caso de ataques inimigos.

Nas décadas de 1970 e 1980, extrapolou a utilização exclusiva para os meios militares, a Internet também foi um importante meio de comunicação acadêmica. Estudantes e professores universitários, principalmente nos EUA, trocavam ideias, mensagens e descobertas pelas linhas de rede mundial.

Todavia, foi somente no ano de 1990 que a Internet começou a alcançar a população em geral. Neste ano, o engenheiro inglês Tim Bernes-Lee desenvolveu a World Wide Web (WWW), possibilitando a utilização de uma interface gráfica e a criação de sites mais dinâmicos e visualmente interessantes. A partir deste momento, a Internet cresceu em ritmo acelerado. Muitos dizem, que foi a maior criação tecnológica a seguir à televisão na década de 1950.

A década de 1990 tornou-se a era de expansão da Internet. Para facilitar a navegação pela Internet, surgiram vários navegadores como, por exemplo, o Netscape e o Internet Explorer, este último da Microsoft de Bill Gates. O surgimento acelerado de provedores de acesso e portais de serviços online contribuíram para este crescimento. A Internet passou a ser utilizada por todos segmentos sociais. Os estudantes passaram a realizar de informações para pesquisas escolares, enquanto jovens utilizavam para a pura diversão em sites de games. As salas de chat tornaram-se pontos de encontro para um bate-papo virtual a qualquer momento. Desempregados iniciaram a busca de empregos através de sites de agências de empregos ou enviando currículos por e-mail. As empresas descobriram na Internet um excelente caminho para melhorar seus lucros e as vendas online dispararam, transformando a Internet em verdadeiros shopping centers virtuais, consolidando a cultura do comercio eletrônico.

Nos dias atuais, é impossível pensar no mundo sem a Internet. Ela tomou parte dos lares de pessoas do mundo todo. Estar conectado na rede mundial passou a ser uma necessidade de extrema importância. A Internet também está presente nas escolas, faculdades, empresas e diversos locais, possibilitando acesso as informações e notícias do mundo em apenas um click.

A INFORMÁTICA E O DIREITO

O direito é por natureza conservador, sendo certo que a introdução de novos princípios e normas exigidos pelos desafios dos novos fatos é lenta e gradual. Há um descompasso entre a ordem jurídica e as transformações sociais, não devendo, distanciar-se com grande intensidade das transformações da sociedade, sob pena de não ser observado voluntariamente. Afinal, o direito eficaz é o direito realmente aplicado e obedecido.

A Internet tem sido utilizada para inúmeras finalidades, seja para realizar negociações comerciais, buscar conhecimento, conhecer pessoas, manter relacionamentos, produzir atividades de marketing pessoal, busca diversão e, em alguns casos, promover transtornos para outras pessoas, incluindo prejuízos financeiros das vítimas. As nossas legislações vem avançando cada vez mais, para que possamos combater este tipo de crimes no ambiente virtual.

Classificação dos crimes de informática

Os crimes virtuais podem ser classificados em crimes próprios e impróprios. Segundo Roberto Antônio Darós Malaquias:

> [...] **Os crimes próprios**: são aqueles que necessitam da internet para ser praticado, ou seja está diretamente relacionado com a utilização da tecnologia da informática e comunicação. Para facilitar a compreensão, tem-se como exemplos enquadrados neste grupo, a criação e disseminação de vírus e outros códigos maliciosos, a negação de serviços, a invasão e a distribuição de dados (público ou privado) e tantos outros atos ilícitos.
>
> **Os crimes impróprios**: são aqueles em que o computador ou a estação de trabalho transforma-se em instrumento para a pratica do delito. Nesse grupo estão inseridos, a título de exemplo, os tipos penais comuns como a calunia, a injuria, a difamação, o furto, o estelionato, a produção, a divulgação e a publicação de fotografias ou imagens contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes e todos os demais delitos preceituados no código penal e nas leis especiais, possíveis de serem praticados com a utilização dessa citada ferramenta e das novas tecnologias.

Crime de informática puro

São aqueles em que o autor visa especificamente ao sistema de informática, em todas as suas formas que compõem a informática são eles o "software", o "hardware", os dados e sistemas contidos no computador, e os meios de armazenamento externo, com pendrive e CDs.

Portanto são aquelas condutas que visam exclusivamente a violar e modificar o sistema de informática da vítima.

As ações físicas se materializam, por exemplo, por atos de vandalismos contra a integridade física do sistema, pelo acesso desautorizado ao computador, pelo acesso indevido aos dados e sistemas contidos no computador.

Portanto, é crime de informática puro toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas.

Crime misto

São todas aquelas ações em que o autor visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação.

Quando o autor objetiva, por exemplo, realizar operações de transferência ilícita de valores de outrem, em uma determinada instituição financeira utilizando-se do computador para alcançar o resultado da vantagem ilegal, e, o computador é ferramenta essencial, defrontamo-nos com um crime de informática misto.

É crime de informática misto porque incidiriam normas da lei penal comum e normas da lei penal de informática. Da lei penal comum, por exemplo, poder-se-ia aplicar o artigo 171 do Código Penal combinado com uma norma de mal uso de equipamento e meio de informática. Por isso não seria um delito comum apenas, incidiria a norma penal de informática, teríamos claramente o concurso de normas (art. 70, CP).

Crime comum

São todas aquelas condutas em que o agente se utiliza do sistema de informática como mera ferramenta a perpetração de crime comum, tipificável na lei penal, ou seja, a via eleita do sistema de informática não é essencial à consumação do delito, que poderia ser praticado por meio de outro recurso.

Como exemplo, os casos de estelionato (art. 171, CP), e as suas mais amplas formas de fraude. Quando o computador é ferramenta escolhida pelo autor, que poderia escolher outros meios diversos da informática. Porém, é de se pensar na possibilidade de qualificadora para o delito de estelionato o uso do sistema de informática.

É aclarar a aplicabilidade aos crimes comuns das normas penais vigentes, porém, atendendo a essa classificação, incorporar ao Código Penal agravantes pelo uso de sistema de informática, vez que é meio que necessita de capacitação profissional e a ação delituosa por esta via reduz a capacidade da vítima em evitar o delito.

Posto isto, entendemos ser a presente classificação apta a elaboração de legislação que possa alcançar os delitos de informática, sem correr o risco de sobreposição de normas, e, assim, também, entendemos que é meio hábil à formação de um eficaz Direito Penal de Informática.

3 SUJEITO DO CRIME

SUJEITO ATIVO

A imputação objetiva ao autor do crime e sua comprovação é extremamente difícil frente à ausência física do sujeito ativo, ocorre que frente à importância da identificação do autor do crime e a dificuldade desta identificação, surgiu à necessidade de se traçar um perfil denominando grupos que praticam determinados crimes virtuais, dentre essas denominações temos a figura do cracker.

> [...] Em princípio, é o criminoso de informática alguém que conhece a vulnerabilidade dos sistemas, dos programas de computadores e de tudo que

> circunda tal ambiente. Deve possuir habilidade de planejar o crime sob esse terreno, percebendo as oportunidades de planejar o crime sob esse terreno, percebendo as oportunidades que facilitam sua prática delitiva e seu anonimato após a descoberta de sua conduta. (LIMA,2007, p.71).

Todavia, não é preciso ser um cracker para se praticar um crime virtual. A facilidade de manipulação e uso da Internet proporcionou que qualquer pessoa, de todas as faixas etárias e camadas sociais, possa ser em potencial um criminoso virtual bastando para isso utilizar a Internet para praticar um comportamento tipificado como crime em nosso ordenamento jurídico.

Vale ressaltar a existência da figura do hacker, que normalmente é injustiçado pela grande mídia que lhe atribuí todas as ações maliciosas do mundo digital. Entretanto, o hacker é um especialista de internet que até conhece e domina as técnicas invasivas, mas não as utiliza para prejudicar ninguém nem obter vantagem indevida. Porém se o hacker mudar de lado e começar a utilizar seus conhecimentos para praticas indevidas ele passará a ser considerado um cracker.

Sujeito Passivo

Quando falamos de um crime específico logo sabemos quem é o sujeito ativo e passivo da conduta, quem realizou e em quem recaiu a ação ou omissão, no caso dos crimes virtuais de forma generalizada a única afirmação cabível é que será sempre uma pessoa física ou jurídica ou uma entidade titular seja pública ou privada titular do bem jurídico tutelado, sempre haverá o sujeito passivo.

Portanto, o sujeito passivo da infração penal pode ser qualquer indivíduo normal, pessoa física, ou até mesmo uma pessoa jurídica, segundo Fabrízio Rosa:

> [...] O Sujeito Passivo, como se sabe, é o ente sobre o qual recai a ação ou omissão realizada pelo Sujeito Ativo. É a pessoa ou entidade titular do bem jurídico tutelado pelo legislador e sobre a qual recai a conduta do Sujeito Ativo. De qualquer modo, o Sujeito Passivo dos “Crimes de Informática” pode ser qualquer pessoas, Física ou Jurídica, de natureza Pública ou Privada. É importante destacar, entretanto, que a maioria desses delitos não chega ao conhecimento das autoridades para a devida apuração em virtude de as

> empresas ou instituições financeiras, por exemplo, terem medo do desprestígio e sua consequente perda da credibilidade que talvez isso possa causar, pois poderá dar a impressão de que ou aquela instituição não possui sistemas de segurança eficazes. E é justamente essa “lei do silêncio” que vem estimulando os criminosos a continuar sua empreitada ilícita. (ROSA, 2002, p.61).

4 QUESTÕES PROCESSUAIS

Tempo do Crime

O Código Penal brasileiro prescreve no artigo 4º a Teoria da Atividade quando versa sobre o tempo do crime. Portanto, não importa qual o momento do resultado provocado por um crime na Internet, o tempo do crime será o momento em que foi efetivamente praticado o delito, assim uma pessoa que envia uma ameaça através de um e-mail e o destinatário somente vem a ler o e-mail meses ou anos após o envio, constará como tempo do crime a época em que este e-mail foi enviado e não o tempo a que ele veio a ser aberto. Em outros casos especiais em que o tempo do crime não será necessariamente o da ação ou omissão. Nos casos de desenvolvimento de páginas da Internet com mensagens difamatórias ou caluniosas contra alguém, enquanto está pagina estiver ativa na Internet, terá que ver o tempo do crime, pois este caso trata-se de crime permanente onde tanto a ação quanto o resultado se prolongam no tempo.

LUGAR DO CRIME

Em relação ao local do crime o Brasil adotou a Teoria da Ubiqüidade de acordo com o que prescreve o artigo 6º do Código Penal Brasileiro, ou seja, o local é onde ocorreu ação ou omissão bem como onde se produziu ou deveria produzir o resultado. Desta forma se o autor de uma ofensa a honra (injúria) a um terceiro se encontra na cidade de Vitória/ES e a vítima das ofensas encontra-se em Cachoeiro de Itapemirim/ES no momento em que tomou conhecimento das ofensas, as duas cidades serão consideradas o lugar do crime. Considerando também lugar do crime, o lugar aonde o servidor que responda as mensagens infringentes está localizado.

TERRITORIALIDADE

No ciberespaço entramos em uma virtualização da realidade, uma migração do mundo real para um mundo de interações virtuais, onde existe uma constante produção, reprodução das relações sociais do espaço. Uma realidade objetiva muitas vezes iniciada no ciberespaço, e que traz consigo um propósito de finalizar-se no mundo real, mais cedo ou mais tarde, direta ou indiretamente, estabelece as trocas identitárias, mesmo não havendo contato físico.

Segundo o nosso Código Penal em seu artigo 5º diz:

> Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.

Competência

Nos crimes cibernéticos, os atos executórios da infração ocorrem em lugares diferentes, e aí está o maior problema em se fixar a competência pois não é fácil de ser determinada uma vez que a Internet rompe fronteiras. Pelo seu caráter transnacional, pode ser que o autor esteja em um país e a vítima em outro. Ou mesmo o fato criminoso pode ocorrer em um local e se consumou em outro completamente diferente.

Os crimes que forem cometidos em diferentes lugares, dentro do território brasileiro, denominam-se delitos plurilocais, já os delitos que se desenvolvem em países diferentes, são chamados de crimes à distância. Com isso temos o artigo 70 do Código de Processo Penal Decreto Lei nº 3.689 de 03 de Outubro de 1941 seus parágrafos 1º e 2º que diz:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.

A competência só será aplicada quando se tratar de casos que não compete a Justiça Federal, que é taxativa e tem previsão legal no artigo 109 da Constituição Federal brasileira:

> Art. 109. Aos juízes federais compete processar e julgar:
> I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho;
> II - as causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País;
> III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional.

5 CRIMINOSOS E ESPECIALISTAS

Tipo de Hackers

O número de crimes virtuais tem crescido, ao mesmo passo em que se populariza o acesso à internet e às redes sociais.

Em tempos em que a privacidade ameaça ruir, é preciso redobrar a atenção e os cuidados para proteger as informações e os dados pessoais e, sobretudo, profissionais.

Normalmente se considera como hacker uma pessoa ou um grupo que ataca para causar danos ou ofensas a qualquer empresa, órgão do governo ou mesmo um computador pessoal. Embora a maneira de operar seja parecida, os objetivos dos hackers são distintos.

> [...] Lammer: é quem está tentando ser hacker, sai perguntando para todo mundo o que fazer para tornar-se um, com isso possui um pouco de conhecimento sobre invasão de sistemas e fica se exibindo na internet por causa disso. É o iniciante;(ROSA, 2002, p.59).

O Lammer na verdade é aquele que se passa por hacker nas redes sociais, e fala sobre coisas que ele vulgarmente diz compreender, mas que na maioria dos casos ele só conhece o que vê em filmes.

Hoje em dia o Lammer evoluiu para uma subcategoria, o Hater, que tem como objetivo promover movimentos negativos sobre um determinado Post ou publicação, pois de forma geral ele não está satisfeito com nada do que é proposto pelo proprietário do conteúdo.

> [...] Preaker: especializados em telefonia, atua na obtenção de ligações telefônicas gratuitas e instalação de escutas, facilitando o ataque a sistema a partir de acesso exterior, tornando-se invisíveis ao rastreamento ou colocando a responsabilidade em terceiros;(ROSA, 2002, p. 59).

Porem hoje as técnicas mais utilizadas por Preaker são os ataques DDOS por negativa de serviço, e é nesta parte que entram os Hactivista. A maioria dos Hactivista, tem como base de ação os ataques por DDOS, derrubando sites e serviços que por alguma razão estão e desacordo com a causa.

Ataques DDOS são na maioria ataques por demanda de pacote, e são mais eficientes quando executado por uma grande quantidade de usuários a um alvo único. Por este motivo os Hactivista são os maiores usuários de Phreaker, pois conseguem movimentar grandes quantidades de trafego a favor da causa.

> [...] Cracker: o mesmo que hacker, com a diferença de utilizar seu conhecimento para o “mal”. Destruir e roubar são suas palavras de ordem. Assim, o cracker usa os seus conhecimentos para ganhar algo; rouba informações sigilosas para fins próprios e destrói sistemas para exibir;(ROSA, 2002, p.59).

Esta classificação é uma das que mais são citadas como sendo o Ruim do lado hacker, e em tese as empresas de comunicação tem razão, pois os Cracker hoje são os principais responsáveis pela descriminação de software e material digital pirata.

O Cracker geralmente trabalha em equipes, onde o grupo em si explora falhas na autenticação de um Software ou serviço a fim de burlar a mesma e obter acesso a Propriedade Intelectual de uma corporação de forma gratuita e ilegal.

Porem hoje em dia é comuns empresas do ramo Digital, contratarem este tipo de serviço, a fim de descobrirem as brechas do seu sistema, e então promover melhorias no método de autenticação do mesmo.

O script Kiddies como o próprio nome já diz, são aqueles usuário que não possuem conhecimento para fazer algo grande, porem sabem utilizar as ferramentas hackers disponíveis na web.

Em geral eles são como os Lammers, pois na maioria não possuem conhecimento avançado no meio digital, mas gostão de se vangloriar por conseguirem atingir pequenos feitos através da execução de Scripts, arquivos em BT ou mesmo sh no caso de sistemas open source Linux.

Na maioria dos casos não são tão perigosos, pois como se tratam de usuários que gostão de reconhecimento, focam seu baixo conhecimento na obtenção de contas de Games e contas de perfil em Redes sociais.

Carder é o pior tipo de Hacker, pois é o que mais causa prejuízo a pessoa física, ou usuário doméstico. Um Carder é unanimo em suas ações, que são focadas no roubo ou obtenção de dados bancários, a fim de efetuar saques, transferências ou mesmo compras utilizando os dados bancários da vítima.

> [...] guru: o “supra - sumo” (mestre) dos hackers. É aquele que tem conhecimentos superiores e grande domínio sobre todos os tipos de sistemas. (ROSA, 2002, p.60).

Como eles atacam

Podemos perceber que nos últimos anos os hackers vem cada vez mais invadindo nosso espaço, jovens inexperientes deixam rastros por onde passam e acabam ganhando seu minuto de fama na mídia. Entretanto temos os hackers profissionais que são cuidadosos para manter seus ataques oculto e de difícil de serem localizados e punidos conforme a lei.

Os hackers tem vários motivos para executar o ato ilícito um exemplo disso é a espionagem industrial que é quando uma empresa contrata um racker para realizar um ataque na empresa concorrente para pegar dados, forma de manejo, formulas de produtos, estratégias de comercialização, temos também os hackers que só querem aprendizado, curiosidade, vingança entre outras coisas.

As formas de executar crimes informáticos são variadas entre elas é o simples ato da pessoa selecionar um arquivo no computador e deletar, como também podem executar de forma mais difícil mais experiente como invadir sistemas de longa distância sem acesso autorizado.

6 CRIMES DE INTERNET

Ao mesmo passo que a Internet sofre modificações diárias, a sociedade passa por uma profunda transformação de suas estruturas, caracterizando-se hoje pela imaterialidade e pela ausência dos limites temporais e espaciais tradicionais. Dessa forma, com o surgimento da informática, seus avanços e popularização, é possível afirmar que a sociedade se encontra diante de uma tecnologia revolucionária e que condiciona o seu funcionamento.

O Direito, pela sua forma dinâmica, também tem sofrido diversas mudanças, na tentativa de acompanhar as evoluções tecnológicas e de se adaptar às transformações sociais, adequando-se, de modo gradual, à nova realidade. Isso porque são necessárias novas soluções para os novos problemas que surgem, o que desperta uma demanda por maior atenção para os aspectos jurídicos do uso do computador, dado o grande desenvolvimento da internet.

Ainda sem a tipificação adequada e com a facilidade de acesso à rede mundial de computadores, os crimes tradicionais previstos em nossa legislação não se mostram suficientes para abranger aqueles cometidos contra o computador ou por meio dele. Em outras palavras, embora ocorra a aplicação do Código Penal para alguns dos crimes cibernéticos, frente ao surgimento de novas modalidades criminosas, se faz necessária uma legislação específica, capaz de englobar com eficiência o maior número possível dessas condutas.

É fundamental que se entenda que a falta de normas especificas é um grande empecilho para a impunidade, já que várias condutas graves continuam sendo atípicas, não podendo ser penalizadas. Algumas medidas emergenciais têm sido adotadas, como a criação de normas próprias que tipificam algumas das condutas criminosas que ocorrem no meio virtual. Esse é o caso das Leis 12.735 e 12.737, ambas de 30 de novembro de 2012, a primeira conhecida popularmente como Lei Azeredo e a segunda como Lei Carolina Dieckmann.

Deste modo é fácil perceber que o mal uso da Internet produz sérias consequências e elevados riscos. Por isso e pela importância que assume atualmente, é evidente que o espaço virtual não deve estar alheio a qualquer forma de regulamentação, sobretudo no que se refere aos temas penais. Tendo em vista a vulnerabilidade do meio informático e o avanço da nova criminalidade, uma sociedade

informada é imprescindível para que se alcance o equilíbrio entre o uso saudável da Internet e a segurança, seja na sua dimensão pública ou pessoal, o que só pode ocorrer a partir do debate e da construção de uma política legislativa mais robusta e que melhor responda às necessidades sociais. Como primeiro passo, é necessária legislação própria e, cabe ao Estado, no desempenho do seu papel de regulador e organizador da sociedade, o dever de buscar mecanismos de prevenção de combate às condutas que infringem a ordem legal estabelecida. E dando aos órgãos competentes recursos para que possam no seu devido papel investigar e punir os criminosos.

7 APLICAÇÃO DO CÓDIGO PENAL EM CONDUTAS PRATICADAS POR MEIO DA INTERNET

O nosso código penal em seu artigo 1º diz “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal”. No entanto, este princípio constitucional, tem sido um obstáculo para se punir os crimes praticados na Internet, no qual, a legislação vem trabalhando para solucionar essas impunidades.

A Lei nº 12.735, de 30 de novembro de 2012 teve o intuito de “tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências”. Já a Lei 12.737/2012 tipifica alguns delitos ocorridos no ambiente cibernético, como a invasão de computadores, produção e disseminação de códigos maliciosos e a clonagem de cartão. Essas leis representam um grande avanço para regulamentação da Internet no país.

A Internet é a primeira tecnologia que a humanidade construiu visando a conectividade global, porém inevitavelmente se confunde o mundo virtual com o mundo real, mas de fato sabemos que a Internet é o conjunto de milhares de redes interligadas entre si espalhadas por todo o planeta.

8 CRIMES CONTRA A VIDA

Homicídio - Art. 121 CPB

Homicídio é o ato de matar uma pessoa, quer seja de forma voluntária ou involuntária. O homicídio é um termo que deriva do latim *homicidĭum* e que se refere à morte de um ser humano causada por outro ser humano. O termo, por sua vez, pode ser usado como sinônimo de assassinato ou crime.

O crime de homicídio no código penal é tipificado simplesmente como “matar alguém”, portanto não importa o meio, seja ele com o auxílio de uma faca, de uma pedra, com as próprias mãos, com uma arma de fogo, por atropelamento utilizando-se de um automóvel ou através da Internet.

Um caso clássico ocorreu em um grande hospital de São Paulo, quando uma pessoa de 45 anos foi internada devido a uma grave crise de diabetes, e o seu desafeto sabendo disso, invadiu o servidor do hospital e fez uma pequena alteração, mudando a prescrição da medicação daquele paciente de insulina para glicose. A enfermeira, agindo com desatenção, imprimiu a prescrição médica e ministrou conforme o documento 50ml de glicose na corrente sanguínea do diabético internado. Em pouco mais de uma hora o paciente veio a óbito devido a uma parada cardíaca. Ficando evidente o nexo causal entre a invasão do sistema com a alteração da medição e a morte do indivíduo, não restando dúvidas que ocorreu nesse caso uma situação em que a Internet foi o meio utilizado para a prática do crime de homicídio.

Induzimento, Instigação e Auxilio a Suicídio - Art. 122 CPB

> [...]O suicídio é a deliberação da própria vida. Suicida, segundo o Direito, é somente aquele que busca direta e involuntária a própria morte. Apesar de o suicídio não ser um ilícito penal, é um fato antijurídico, dado que a vida é um bem público indisponível (CAPEZ, 2017, p. 117).

A Internet é mais um meio de se praticar o delito, podemos encontrar comunidades, grupos nas redes sociais e até em sites específicos que ensinam a cometer suicídio, esses sites dispõem informações e instruções sobre como auxiliar nas referidas práticas. Recentemente temos ouvido falar sobre o jogo Baleia azul, uma

tradução direta do nome original russo, Siniy Kit, que foi criado no ano de 2013 na Rússia pelo o russo Philipp Budeikin, de 21 anos, o jogo foi criado para incitar o suicídio. Em uma reportagem no site Último segundo IG São Paulo publicada no dia 10/05/2017 diz: Philipp Budeikin, que está aguardando julgamento, confessou ter incitado o suicídio de 16 garotas e afirmou à polícia que suas vítimas eram "resíduo biológico".

O jogo letal Baleia Azul é um processo de lavagem cerebral de adolescentes vulneráveis ao longo de 50 dias. Os jovens devem realizar 50 tarefas como acordar de madrugada, assistir a filmes de terror e praticar automutilação. O último comando do jogo é o suicídio, os jovens são monitorados pelo “curador” que está à espera de fotos ou vídeos da vítima para confirmação que foi executado os comandos, se caso a vítima se recusar a fazer as tarefas que o curador pediu elas são ameaçadas.

Lesões corporais - Art. 129 CPB

O crime de lesão corporal por trata-se de modalidade de menor potencial ofensivo por vezes é abraçada por uma ação de maior gravidade. Entretanto, quando evidenciado isoladamente, requer características próprias.

A lesão corporal também está no meio virtual pois é possível ser o autor de um crime através da Internet e é possível praticar lesões corporais de natureza culposa. Existe vários sites com diversos conteúdos, em alguns deles ensina as pessoas a manipularem substâncias perigosas. Seria responsabilizado pela pratica de lesões corporais o autor de um site que fala sobre manipulação de explosivos e materiais inflamáveis, caso alguém incentivado e orientado por este viesse a se ferir em seus experimentos.

9 CRIMES CONTRA A HONRA

Os crimes contra a honra estão previstos nos artigos 138, 139 e 140 do Código Penal, sendo que os mesmos são crimes comuns na Internet, tendo em vista o alto número de usuários que navegam diariamente na rede.

> [...] Honra são as qualidades de um indivíduo físicas, morais e intelectuais, fazendo-a respeitada no meio social onde se convive, a qual diz respeito ainda à sua autoestima. A honra é um patrimônio que a pessoa possui, sendo que o mesmo deve ser protegido, tendo em vista que os seus atributos como pessoa em sociedade irá definir a sua aceitação ou não para conviver em um determinado grupo social (CRESPO, 2011, p.90).

Os crimes contra a honra subdividem-se entre Calúnia, Difamação e Injúria estão em ordem decrescente de gravidade.

Recentemente chegou ao Brasil e no Espirito Santo o aplicativo Sarahah esse aplicativo foi criado na Arábia Saudita que significa “franqueza” e “honestidade”, e o seu objetivo é o usuário dizer franquezas e honestidade para um colega do serviço ou amigo sendo que as mensagens são anônimas.

O investigador da Delegacia de Repressão aos Crimes Eletrônicos do Espírito Santo (DRCE), Eduardo Pinheiro, é quem fala de algumas ressalvas sobre o aplicativo. Atenção, que ele não é tão anônimo assim!

> "O aplicativo Sarahah, recentemente lançado no Brasil, com o slogan - obtenha comentários honestos de seus colegas de trabalho e amigos -, possibilita que uma pessoa possa enviar mensagens para outras de forma anônima, brindando o remetente da mensagem contra a timidez ou a vergonha. Por outro lado o app é visto com muito receio por especialistas da área devido ao fato de poder ser utilizado para envio de ofensas pessoais, mentiras, falsos boatos e ameaças, caracterizando aí um crime virtual.
> É bom lembrar que em 2014 um aplicativo semelhante, de nome Secret, após muitos casos envolvendo o app terem se tornado caso de polícia, acabou sendo bloqueado pela justiça brasileira, sob o argumento de que a Constituição Federal veda o anonimato. Todavia, é bom ressaltar que o anonimato oferecido pelo aplicativo só é válido entre os usuários, uma vez que em todas as postagens são armazenadas no servidor do Sarahah com os dados de conexão do usuário, que poderão ser fornecidos para a justiça caso ocorra um comportamento abusivo ou criminoso nessa nova rede social”. (PINHEIRO, 2017)

Calúnia – Art. 138 CPB

No crime de Calúnia a honra objetiva da vítima é abalada, ou seja, o agente atribui à vítima a prática de fato definido como crime, sabendo que a imputação é falsa, abalando assim, sua reputação perante a sociedade.

A calúnia pode ocorre em qualquer lugar, hoje em dia a calúnia é muito vista nas redes sociais como facebook, salas de bate-papo, instagram, twiter, whatsapp e entre outros sites, para ser considerado calúnia o autor deve imputar a alguém um fato tido como crime e ser posto no ambiente virtual, carta, jornal ou por suas próprias palavras. O autor será responsabilizado ao divulgar esse fato falsamente vindo a responder pelo crime nas formas da lei.

Difamação – Art. 139 CPB

A difamação é quando alguém cria uma má fama para outra pessoa, prejudicando assim a reputação desta. No Código Penal Brasileiro, a difamação é crime definido pelo ato de desonrar alguém divulgando informações a respeito da outra, gerando descrédito de sua imagem pública. A difamação é qualificada como um dos crimes contra a honra.

Difamação é um termo jurídico que consiste em atribuir a alguém fato determinado ofensivo à sua reputação, honra objetiva, e se consuma, quando um terceiro toma conhecimento do fato. Segundo o autor Gabriel Cesar Zaccaria de INELLAS

> [...] O crime de Difamação e praticado na internet nas suas mais diversas formas, seja na perpetuação de e-mails enviados a pessoas diversas da vítima, imputando à esta, algum fato que ofenda sua honra objetiva, ou publicando em redes sociais as mesmas ofensas. No crime de Difamação a pessoa Jurídica não pode ser sujeito passivo, tendo em vista que no art. 139 do CP a norma é dirigida à pessoa humana, mas, quando o crime for praticado por meio da imprensa, pode-se aplicar a Lei nº 5.250/67 – Lei de Imprensa. (INELLAS, 2004, p.51).
>
> [...] Na Difamação a lei não exige que a atribuição seja falsa, basta somente à perpetuação de algo que venha a ofender a reputação do agente perante a sociedade, o crime irá se consumir no momento em que o terceiro tomar conhecimento do fato, em ambiente virtual o crime irá se consumir, por exemplo, quando alguém espalhar um ato ofensivo a uma pessoa pelas redes sociais, e os usuários presentes fizeram a leitura do fato ofensivo (PINHEIRO, 2010, p.91).

Injúria- Art. 140 CPB

A injúria é um crime que consiste em ofender verbalmente, por escrito, via redes sociais ou até fisicamente, a dignidade ou o decoro de alguém, ofendendo a moral, com a intenção de abater o ânimo da vítima.

O crime de injúria consiste na propagação de qualidade negativa da vítima por um terceiro, qualidade esta que diga respeito aos seus atributos morais, intelectuais ou físicos, afetando de forma significativa a honra subjetiva da vítima.

A câmara dos Deputados aprovou, um projeto de lei de Nº 5.555-A de 2013 (Do Sr. João Arruda) que torna crime a vingança virtual, com a divulgação e a exposição pública da intimidade sexual mais conhecido como "envio de nudes".

O projeto aprovado prevê pena de reclusão de 3 meses a 1 ano, que pode ser aumentada de um terço à metade se por motivo torpe ou contra pessoa incapaz.

> “Segundo a advogada Flávia Guth, que assina a coluna Pensar Direito no site Metrópoles, a lei foi proposta em 2012 e se enquadra como crime quaisquer violações de segurança de dispositivos eletrônicos — sejam computador, celular ou tablet e etc. A premissa é de que a distribuição indevida de imagens ou vídeos não autorizados pela vítima categoriza crime digital, mas ainda é enquadrado na categoria a invasão de e-mail, transgressão de propriedade intelectual, disseminação de vírus e fraudes bancárias”.(GUTH, 2017).

Ressalta ainda que o canal online Safernet auxilia vítimas de crimes digitais que tenham suas fotos vazadas. A chamada “Helpline” funciona como uma rede de auxílio que pode ser acessada via e-mail ou chat no site oficial. Tendo três orientadores.

Segundo o portal oficial, a equipe conta com suporte governamental, parcerias com a iniciativa privada e autoridades policiais e judiciais. O objetivo é aconselhar a vítima que esteja passando por situações como humilhações, intimidações, chantagem, tentativa de violência sexual ou exposição forçada em fotos ou filmes sensuais.

O site auxilia também crianças e adolescentes que estão sofrendo ciberbullying. Os atendimentos são gratuitos e o número máximo de orientações pelo chat ou pelo e-mail é de 4 (quatro) encontros. A partir do segundo encontro, será preciso um termo de autorização dos pais para a continuidade da orientação de criança ou adolescente, conforme determina o Art. 8º do Código de Ética Profissional do Psicólogo.

Para as pessoas que gostam de compartilhar sua intimidade nas redes sociais. O Coding Rights, um Think-and-Do tank criado para promover o entendimento e contribuir para a proteção e promoção de Direitos Humanos no mundo digital, elaborou o zine Safer Nudes Guia Sensual de Segurança Digital, com dicas para quem quiser mandar nudes sem riscos de se expor além do planejado. O guia traz questões sobre o direito à privacidade e também sobre o direito de decidir sobre o próprio corpo e a própria imagem.

10 CRIMES CONTRA A LIBERDADE INDIVIDUAL

Constrangimento ilegal – Art.146 CPB

O crime de constrangimento ilegal tem sido rotineira já que temos a Internet com um meio de viabilizar essa pratica.

Consuma-se o crime quando a vítima, submetida ao constrangimento, toma o comportamento a que foi obrigada, fazendo o que não desejava ou fazendo o que queria. É possível a tentativa, que ocorre quando o ofendido não cede à vontade do ofensor.

Ameaça - Art.147 CPB

A ameaça se diferencia do constrangimento ilegal, porque neste o agente busca uma conduta positiva ou negativa da vítima já a ameaça, o autor pretende tão somente atemorizar o sujeito passivo. A ameaça tem que ser admissível, por obra humana, capaz de instituir receio, independente de causar ou não dano real a vítima e a Internet é mais um meio de se praticar o crime de ameaça.

Violação de correspondência – Art. 151 CPB

A ação do crime de violação de correspondência, se dá quando o autor abre uma correspondência que não é sua, não sendo dirigida a ela, simplesmente na intenção de olhar, ver, ler, tomar conhecimento do seu teor. Então essa ação se da como uma invasão.

A recente Lei 12.737, de 30 de novembro de 2012, publicada no DOU (diário oficial da união) de 3 de dezembro do mesmo ano, tipificou um novo crime denominado Invasão de Dispositivo Informático, previsto no artigo 154-A, do Código Penal, que entrará em vigor após 120 dias de sua publicação oficial, ou seja, em 3 de abril de 2013.

Mesmo antes de a referida lei ser publicada e sancionada, o respectivo Projeto de lei nº 35/2012 já havia recebido o apelido de “Carolina Dieckmann”, em razão da repercussão do caso amplamente divulgado pela mídia no qual a atriz brasileira (reconhecida por suas atuações em diversas telenovelas e seriados da Rede Globo) teve seu computador invadido e seus arquivos pessoais subtraídos, inclusive com a publicação de fotos íntimas que rapidamente se espalharam pela internet através das redes sociais. Consequentemente, o fato gerou intensa pressão social para a criminalização, em regime de urgência, dessas condutas que até então não eram previstas como crime em espécie pelo Código Penal.

Violação de segredo profissional – Art. 154 CPB

Consuma-se o crime de revelação de segredo profissional quando o segredo é revelado a uma só pessoa, sendo a tentativa possível. A intenção do autor é revelar e não divulgar. A ação típica consiste em revelar, total ou parcialmente, o segredo de que o autor teve conhecimento em razão de função, ministério, ofício ou profissão, não sendo necessário que o segredo preexista às relações entre o autor o interessado em sua conservação.

Vejamos uma jurisprudência do Tribunal de Justiça que diz:

> TJ-CE - Habeas Corpus HC 06282641420158060000 CE 0628264-14.2015.8.06.0000 (TJ-CE)
> Data de publicação: 17/02/2016
> Ementa: HABEAS CORPUS. PENAL E PROCESSO PENAL. TORTURA. CALÚNIA. DIFAMAÇÃO. INJÚRIA. CONSTRANGIMENTO ILEGAL. AMEAÇA. DIVULGAÇÃO DE SEGREDO. VIOLAÇÃO DO SEGREDO PROFISSIONAL. DENUNCIAÇÃO CALUNIOSA. COAÇÃO NO CURSO DO PROCESSO. EXERCÍCIO ARBITRÁRIO DAS PRÓPRIAS RAZÕES. TRANCAMENTO DE AÇÃO PENAL. MATÉRIA NÃO DISCUTIDA NO JUÍZO A QUO. SUPRESSÃO DE INSTÂNCIA. ORDEM NÃO CONHECIDA. 1. Evidenciado que o impetrante não submeteu os questionamentos insculpidos na inicial, que embasam o pleito concernente ao trancamento da ação penal, originariamente, ao Juiz do caso, que aqui figura como autoridade impetrada, torna-se inviável a manifestação direta por este Tribunal, sob pena de laborar

> per saltum, suprimindo um grau de jurisdição. Precedentes. 2. Ordem não conhecida. ACÓRDÃO: Vistos, relatados e discutidos estes autos, acorda a 1ª Câmara Criminal do Tribunal de Justiça do Estado do Ceará em, à unanimidade e dissonância com o parecer da PGJ, não conhecer da ordem de habeas corpus, nos termos do voto da relatora. Fortaleza, 16 de fevereiro de 2016. Presidente do Órgão Julgador DESA. LÍGIA ANDRADE DE ALENCAR MAGALHÃES Relatora.

Invasão de dispositivo informático Art. 154-A CPB

A Lei Carolina Dieckmman tipificou o Art. 154-A do Código Penal: “Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.”

Porém para que exista a caracterização desde crime é preciso que devido a invasão o agente obtenha, altere ou destrua dados e que o dispositivo invadido possua algum recurso técnico de segurança (Firewall, senhas, etc). A mera invasão sem alteração do sistema invadido não caracteriza o crime de invasão de dispositivo informático, pois assim desejou o legislador pátrio.

11 CRIMES CONTRA O PATRIMÔNIO

Furto – Art.155 CPB

O artigo 155 do código penal diz: “Subtrair, para si ou para outrem, coisa alheia móvel”. O furto tem sido uma pratica comum no meio digital pois os autores desses crimes agem de forma silenciosa com o conhecimento avançado na informática. Os autores fazem desvios de dinheiro da conta da vítima para a conta de terceiros ou para si próprio, furto de banco de dados privados, furto de arquivo entre outras ações.

Geralmente o furto de quantias em dinheiro de contas bancárias pelas internet são caracterizados pelo crime de furto qualificado, sendo a destreza a qualificadora.

Extorsão – Art. 158 CPB

A pratica de extorsão é o ato de obrigar alguém a tomar um determinado comportamento, por meio de ameaça ou violência, com a intenção de obter vantagem, recompensa ou lucro. Na Internet a extorsão é possível quando o autor do crime constrange a vítima por vias de redes sociais.

O Extorsão vem expressa no artigo 158 do Código penal que diz: “Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa”.

Atualmente a Internet tem sido cada vez mais utilizada para a prática do crime de extorsão. Muitas vezes o agente utiliza uma informação ou uma foto íntima da vítima para exigir quantia em dinheiro para não realizar a divulgação pela Web.

Mais recentemente a ação de crackers que invadem computadores e criptografam os dados da vítima com códigos maliciosos do tipo “ransomware” e a seguir pedem resgate a ser pago com o dinheiro digital “bitcoin” para que os dados da vítima sejam devolvidos. Muito embora o pagamento do valor do resgate não dá nenhuma garantia que a chave que libera o acesso aos dados será realmente enviado para a vítima.

Dano - Art. 163 CPB

A maioria dos crimes ou delitos possui uma característica em comum, ou seja, o fato de significarem dano à vítima. A expressão pressupõe uma perda ou diminuição de um bem jurídico, ainda que momentaneamente.

O dano pode ser causado de diversas forma e uma delas pode ser um vírus dentro de um e-mail que quando a vítima abrir o mesmo tende a disseminar vírus em seu computador vindo causar um dano.

Estelionato - Art.171 CPB

A figura do estelionato é caracterizada pelo emprego de meios fraudulentos, induzindo alguém em erro, para obtenção de vantagem ilícita. Consiste

no fato de quem, por meio enganoso, causa dolosamente injusto dano patrimonial a outrem. Desta forma, melhor se moldaria o tipo, para se enquadrar na esfera da informática, na figura da fraude informática, onde esta seria a lesão ao patrimônio por meio enganoso, consumando-se, também, com o alcance da vantagem ilícita, em prejuízo alheio.

As condutas variam conforme o uso que o agente faz dos meios eletrônicos disponíveis, com o fim de atingir um objetivo, um dos crimes mais populares tanto na internet quanto fora dela é o estelionato o código penal em seu artigo 171,caput, que:

> Artigo. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artificio, ardil, ou qualquer outro meio fraudulento, pena- reclusão de 1(um) a 5 (cinco) anos e multa.

No caso da aplicação do estelionato no meio informático, a conduta do agente será de induzir ou manter a vítima em erro, e com isso, obtendo vantagem ilícita, para si ou para outrem. Diversas são condutas dos estelionatários na internet, a questão é tipificar-las como estelionato, o legislador previu, com meio executório a fraude com objetivo de obter consentimento da vítima, iludi-lá para que voluntariamente entregue o bem, o agente leva a vítima a erro, enganando a mesma, mantendo-a em erro.

Uma das condutas típicas do estelionato pela Internet consiste no agente encaminhar e-mails com conteúdo falso ao usuário, induzindo o mesmo a clicar em links disponíveis no corpo do e-mail, técnica chamada phishing, em que muitas vezes direciona o usuário para um site falso onde o mesmo digita informações pessoais ao agente que formulou a pagina falsa, estas informações são enviadas ao agente por meio da Internet, que após apropriar-se dos seus dados bancários, transfere os valores disponíveis em conta para o seu domínio.

12 CRIMES CONTRA OS COSTUMES

Facilitação a prostituição – Art. 228 CPB

> [...] A prostituição é considerada uma das “profissões” mais antigas da história da humanidade. Alguns chegam até mesmo a dizer que se trata de um “mal necessário”, pois a sua existência impede, por exemplo, o aumento do número de casos de violências sexuais. (GRECO, 2017, p.149).

O favorecimento da prostituição ou outra forma de exploração sexual está empregada no nosso Código Penal Brasileiro que diz:

> Artigo 228. Induzir ou atrair alguém à prostituição ou outra forma de exploração sexual, facilitá-la, impedir ou dificultar que alguém a abandone: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa.
> § 1º Se o agente é ascendente, padrasto, madrasta, irmão, enteado, cônjuge, companheiro, tutor ou curador, preceptor ou empregador da vítima, ou se assumiu, por lei ou outra forma, obrigação de cuidado, proteção ou vigilância: Pena – reclusão, de 3 (três) a 8 (oito) anos.
> § 2.º Se o crime é cometido com emprego de violência, grave ameaça ou fraude, reclusão, de 4 a 10 anos, além da pena correspondente à violência.
> 3.º - Se o crime é cometido com o fim de lucro, aplica-se também multa.

Neste tipo pena, não se caracteriza como crime hediondo por se tratar de maior de 18 anos. Com tudo um exemplo disso é o site www.ilhadoprazer.com.br esse site é do Estado do Espirito Santo estando ativo a mais de 10 anos, tendo o conteúdo de favorecer, facilitar a prostituição, nele é possível ver fotos, divulgar fotos e contratar on-line os serviços nele disponibilizados. No entanto os responsáveis desse site praticam o favorecimento, facilitação da prostituição.

Rufianismo – Art. 230 CPB

No Brasil, a lei não impede que uma pessoa faça sexo em troca de dinheiro nem que ela faça publicidade dessa atividade. Jornais, revistas e sites por exemplo, anunciam os serviços oferecidos por acompanhantes de todos os sexos de maneira legal. O rufianismo está presente no nosso Código Penal Brasileiro que diz:

> Art. 230 - Tirar proveito da prostituição alheia, participando diretamente de seus lucros ou fazendo-se sustentar, no todo ou em parte, por quem a exerça:

> Pena - reclusão, de um a quatro anos, e multa.
> § 1o Se a vítima é menor de 18 (dezoito) e maior de 14 (catorze) anos ou se o crime é cometido por ascendente, padrasto, madrasta, irmão, enteado, cônjuge, companheiro, tutor ou curador, preceptor ou empregador da vítima, ou por quem assumiu, por lei ou outra forma, obrigação de cuidado, proteção ou vigilância: Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 2o Se o crime é cometido mediante violência, grave ameaça, fraude ou outro meio que impeça ou dificulte a livre manifestação da vontade da vítima: Pena - reclusão, de 2 (dois) a 8 (oito) anos, sem prejuízo da pena correspondente à violência.

Tipificando essa conduta como crime.

13 PORNOGRAFIA INFANTIL

A Internet é, sem dúvida, o maior avanço tecnológico de todos os tempos. A princípio sua função era interligar pessoas no mundo inteiro de forma construtiva e saudável, mas, nos últimos anos serviu como a principal ferramenta de demonstração de diversas ideias, inclusive, ideias perversas como o movimento pró-pedofilia.

Vários pedófilos utilizam o ambiente da internet para divulgar suas experiências através de grupos no facebook, grupos de whatsapp e sites, para compartilhar seus supostos direitos, estabelecerem regras de como deve se comportar diante das crianças e disponibilizar fotos e vídeos.

Por não haver fronteiras na rede mundial de computadores, a Internet se tornou um lugar propício para os pedófilos, um meio democrático, barato, e rápido de se comunicar além de permitir mudanças constantes de site e e-mail. Assim se tornando impossível controlar a pratica dos pedófilos.

Alguns países possuem leis proibindo o uso da Internet para recrutar menores com a intenção de realizar o ato sexual, virtual ou não.

O pedófilo não se distingue na sociedade pela aparência, na Internet ele pode se passar por outra criança para ganhar a confiança da vítima e está por sua vez, ainda imatura e inocente, acredita e passa a confiar em seu novo “amiguinho” que na verdade é um sujeito sem escrúpulos. Daí a importância da presença dos pais.

Um exemplo disso é uma reportagem que foi divulgada no site G1.com dia 09/03/2017 sobre “Pedófilo australiano é indiciado por 931 crimes após se passar pelo cantor Justin Bieber”, o acusado Gordon Douglas Chalmers de 42 anos de idade é um professor de direito na faculdade de tecnologia de Queensland, e foi detido em novembro suspeito de ter cometido 931 crimes de pedofilia, depois que autoridades

da Alemanha e dos Estados Unidos alertaram seus colegas do Estado australiano de Queensland. A polícia revistou a casa de Chalmers na cidade de Brisbane e o acusou de usar servidores para se conectar com menores de 16 anos para ter acesso a material pornográfico infantil.

O mesmo persuadia crianças e adolescentes para enviar fotos explicitas se passando pelo cantor canadense Justin Bieber.

O telefone celular é outro meio muito usado pelos jovens nos dias de hoje, muitas vezes usando de má-fé. Jovens tiram fotos comprometedoras o famoso “nudes” e postam em redes sociais alimentando ainda mais a mente perversa e obsessiva dos pedófilos.

O papel da mídia é muito importante na defesa dos direitos da criança e adolescente, mas, na busca de audiência, e mesmos sujeitos ao código de conduta e de ética, levam ao ar cenas que induzem à erotização precoce.

Há um grave aumento no número de casos de violência sexual contra crianças e adolescentes, nos últimos anos o fator contribuinte para esse aumento foi à disseminação de informações sobre o tema nos meios de comunicação.

Visando oferecer maior proteção ao uso da internet, foi criado a Central Nacional de Denúncias de Crimes Cibernéticos, que é constituído em um sistema automatizado de gestão de denúncias com parceria do Ministério Público Federal com a Polícia federal e a Secretaria Especial dos Direitos Humanos da presidência da República. Em 2007 os Conselhos Estaduais da Criança e do Adolescente, com a coordenação nacional da Secretaria Nacional dos Direitos Humanos, lançou uma ampla campanha para coibir a prática de crimes contra menores, através de denúncias anônimas.

O artigo 234 do Código Penal - Decreto Lei 2848/40 diz:

> Art. 234 - Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno: Pena - detenção, de seis meses a dois anos, ou multa.
> § 1º. Incorre na mesma pena quem:
> I - vender, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
> II - realizar, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
> III - realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

O elemento subjetivo do tipo é o dolo, o qual o agente tem a finalidade de expor ao público, ou comercializar o objeto material do crime, não é necessário que alguém venha a ter acesso ao material para que o crime venha a ser consumir, basta somente a disponibilização do material a possibilidade de que venha a ter acesso ao mesmo.

Há que se fazer uma distinção entre a pedofilia e a pornografia infantil, naquela há uma perversão sexual, a qual o adulto experimenta sentimentos eróticos com crianças e adolescentes, já na pornografia infantil não é necessário a ocorrência da relação sexual entre adultos e crianças, mas sim, a comercialização de fotografias eróticas ou pornográficas envolvendo crianças e adolescentes.

O estatuto da criança e do adolescente (ECA), lei 8.069/90 estabelece algumas penalidades para o pedófilo e aquele que divulgar ou comercializa imagens, vídeos envolvendo crianças em cena de sexo.

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente: Pena - reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I- no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II- prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade;
> III - prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena 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 pornográfica envolvendo criança ou adolescente: Pena - reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre 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 cena de sexo explícito ou

> pornográfica 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, 241-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 funcionários responsáveis 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.
> 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 visual:
> Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, pública 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 a se exibir de forma pornográfica ou sexualmente explícita.
> 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.

Para coibir esse crime o presidente da República Michel Temer sancionou a lei que foi publicado no Diário Oficial da União (DOU) no dia 09/05/2017, a Lei Nº 13.441, que acrescenta ao Estatuto da Criança e do Adolescente, as regras de infiltração de policiais na Internet para coibir crimes de exploração sexual. Requerida pelo Ministério Público ou representação de autoridades policial, a atuação dos agentes será de até 90 dias, com possibilidade de renovações com prazo máximo de 720 dias.

A infiltração não será admitida se a prova puder ser obtida por outros meios, e as informações coletadas deverão ser encaminhadas diretamente ao juiz responsável, que zelará por seu sigilo.

Além disto, a lei diz que “não comete crime o policial que oculta a sua identidade para, por meio da Internet, colher indícios de autoria e materialidade dos crimes”.

Segundo o dispositivo legal, tanto a autoridade judicial como o Ministério Público poderão solicitar relatórios parciais sobre a infiltração. Os documentos deverão conter dados cadastrais e de conexão do usuário, como endereço de Protocolo de Internet, local e horário de acesso à rede.

A medida será admitida apenas em casos que não ofereçam um modo alternativo de obtenção de provas. As informações apuradas serão remetidas diretamente ao juiz responsável por autorizar a operação.

De 2007 a 2016, a central da organização não governamental (ONG) SaferNet registrou mais de 3 milhões de denúncias de diversas naturezas, como crimes de tráfico de pessoas, racismo, xenofobia, intolerância religiosa e maus tratos aos animais. Do total, foram reportadas e processadas 1.518.617 de denúncias anônimas de pornografia infantil, que envolviam 312.037 páginas online distintas, das quais 17.918 eram brasileiras.

14 FORMA DE COMBATER OS CRIMES VIRTUAIS

O Brasil está cada vez mais presente na rota dos ciberataques e fraudes na Internet. Nos últimos dois anos, os dados mostraram-se desfavoráveis ao evidenciarem no País um número crescente de crimes virtuais relacionados ao furto de números de cartões de créditos, senhas bancárias e furtos de dados pessoais.

O combate aos crimes no mundo virtual pode ser feito de diversas forma uma delas é cada um ser vigilante do seus atos na Internet, a maior parte dos crimes cometido é de direta participação da vítima. Então cabe a cada indivíduo ser vigilante no ambiente virtual.

Outra forma de combate é a participação do governo disponibilizando estrutura decente para que os órgãos competentes possam seguir com todas investigações.

Marcos Civil da Internet

Marco Civil da Internet é uma lei que normatiza os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso da Internet no Brasil. O poder executivo apresentou seu projeto de Lei nº 2.126 de 2011, e posteriormente foi aprovado no dia 25/03/2014 na Câmara dos Deputados sendo materializada na Lei nº 12.965, de 23 de abril de 2014.

O Marco Civil da Internet é o nome popular que foi dada a Lei nº 12.965, de 23 de abril de 2014 conhecida por “Constituição da Internet”, e é responsável por estabelecer os princípios e garantias normativas do convívio civil na rede mundial online de computadores. Essa lei foi “solicitada em caráter de urgência pela Presidência da República após um fato que veio à tona em todos os meios de comunicação que um ex-técnico da CIA Edward Snowden, de 29 anos, foi acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana, utilizando servidores de empresas como Google, Apple e Facebook e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da ex presidente Dilma Rousseff com seus principais assessores”.

O Marco Civil da Internet, como o próprio nome faz supor, não criminaliza nenhum comportamento no mundo virtual, apenas legisla na esfera administrativa e civil.

Uma das principais novidades foi o Decreto 8.771/2016, de 11 de maio e com *vacatio legis* de 30 dias, portanto com vigência a partir de 10 de junho, que regulamentou o Marco Civil da Internet “para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações”. Porém, o Decreto ainda tem sido muito pouco observado e aplicado pela jurisprudência, com não muito mais que algumas dezenas de citações até o presente.

Infiltração de Agente da polícia na Internet Lei 13.441/17

A Lei nº 13.441/17 insere no Estatuto da Criança e do Adolescente os artigos 190-A, B, C, D e E, para dispor a respeito da infiltração virtual de agentes policiais com a finalidade de investigar delitos relativos à dignidade sexual de crianças e adolescentes, cujos atos de execução, ou mesmo preparatórios, sejam cometidos pela internet.

Os crimes cuja investigação enseja a infiltração virtual são aqueles relativos à pornografia envolvendo crianças e adolescentes, abrangendo-se todas as formas tipificadas na Lei nº 8.069/90, ou seja, a produção e a distribuição do material, a aquisição e o armazenamento, a simulação da participação em cenas de sexo explícito e o aliciamento para praticar ato libidinoso com criança. Além disso, permite-se a infiltração virtual para investigar os crimes de invasão de dispositivo informático, estupro de vulnerável, corrupção de menores, satisfação de lascívia mediante presença de criança ou adolescente e favorecimento da prostituição ou de outra forma de exploração sexual de criança ou adolescente ou de vulnerável.

Segundo o caput do Art. 190-A, a infiltração se dá por agentes de polícia. Como “agentes de polícia” devem ser entendidos os membros das corporações elencadas no Art. 144 da Constituição Federal, a saber: Polícia Federal propriamente dita, rodoviária e ferroviária; e Polícia Estadual (civil, militar e corpo de bombeiros), observadas, nesta última hipótese, a organização própria de cada unidade da federação. Mas nem todos estes órgãos possuem atribuições investigativas. Com efeito, o inciso I, deste dispositivo constitucional atribui à polícia federal a tarefa de apurar infrações penais. Já o inciso IV, § 4º do Art. 144 da CRFB, comina às polícias civis estaduais essa tarefa investigativa. São, portanto, os policiais federais e civis aqueles habilitados a servirem como agentes infiltrados. Veda-se, destarte, que, por exemplo, agentes do Ministério Público atuem como infiltrados. Ou membros de Comissões Parlamentares de Inquérito, de Corregedorias em geral e, ainda, das receitas federais ou estaduais. Também os componentes do Sistema Brasileiro de Inteligência (Sisbin) e da Agência Brasileira de Inteligência (Abin), não podem se infiltrar.

15 CONSIDERAÇÕES FINAIS

Buscou-se, desde o princípio, explicar sobre os crimes virtuais, considerando tantos os crimes que efetivamente se encontram tipificados em nosso ordenamento jurídico penal Brasileiro, quanto aquelas condutas que, mesmo não tendo tipificação causam danos graves à sociedade.

Os crimes virtuais, vem se tornando cada vez mais frequentes, graças ao uso constante da Internet pela sociedade propiciaram o surgimento de novos tipos penais, bem como novas formas de praticar crimes já conhecidos. Fácil a percepção de que a informática se tornou um meio eficaz para execução de tipos penais.

Através da pesquisa bibliografia realizada, denota-se tratar de um assunto extremamente atual, podendo-se perceber que a legislação acerca da informática era bastante escassa em nosso país. No entanto nosso ordenamento jurídico, principalmente a legislação penal, vem se adaptando para prevenir que condutas que lesem os princípios e os valores da sociedade brasileira sejam repelidas.

As Leis 12.735 e 12.737, ambas de 2012, inovaram o cenário jurídico Penal, além da Lei 12.965 de 2014, que vem regular o uso da Internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, em respondendo à aflição da sociedade e dos aplicadores da lei, que presenciavam fazer, haja vista a falta de previsão legal, ficando os agentes criminosos isentos de pena.

É importante salientar que as leis têm o condão de acabar com os crimes virtuais. A progressão da criminalidade no mundo virtual requer outras providências por parte do Estado, dirigidas à sua apuração e repressão de forma eficaz. Mas para que os profissionais possam investigar eles precisam ter equipamentos modernos para enfrentar as destrezas dos infratores, esses que muitas vezes são profissionais da área de informática ou pessoas com alto conhecimento técnico, que facilitam a sua atuação e dificultam a sua identificação.

16 ANEXOS

Lei de Interceptação Telefônica Lei nº 9.296, de 24 de Julho de 1996.

LEI Nº 9.296, DE 24 DE JULHO DE1996.

Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.

Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática.

Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:

I - não houver indícios razoáveis da autoria ou participação em infração penal;

II - a prova puder ser feita por outros meios disponíveis;

III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.

Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:

I - da autoridade policial, na investigação criminal;

II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Art. 4° O pedido de interceptação de comunicação telefônica conterá a demonstração de que a sua realização é necessária à apuração de infração penal, com indicação dos meios a serem empregados.

§ 1° Excepcionalmente, o juiz poderá admitir que o pedido seja formulado verbalmente, desde que estejam presentes os pressupostos que autorizem a interceptação, caso em que a concessão será condicionada à sua redução a termo.

§ 2° O juiz, no prazo máximo de vinte e quatro horas, decidirá sobre o pedido.

Art. 5° A decisão será fundamentada, sob pena de nulidade, indicando também a forma de execução da diligência, que não poderá exceder o prazo de quinze dias, renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova.

Art. 6° Deferido o pedido, a autoridade policial conduzirá os procedimentos de interceptação, dando ciência ao Ministério Público, que poderá acompanhar a sua realização.

§ 1° No caso de a diligência possibilitar a gravação da comunicação interceptada, será determinada a sua transcrição.

§ 2° Cumprida a diligência, a autoridade policial encaminhará o resultado da interceptação ao juiz, acompanhado de auto circunstanciado, que deverá conter o resumo das operações realizadas.

§ 3° Recebidos esses elementos, o juiz determinará a providência do art. 8° , ciente o Ministério Público.

Art. 7° Para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público.

Art. 8° A interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, preservando-se o sigilo das diligências, gravações e transcrições respectivas.

Parágrafo único. A apensação somente poderá ser realizada imediatamente antes do relatório da autoridade, quando se tratar de inquérito policial (Código de Processo Penal, art.10, § 1°) ou na conclusão do processo ao juiz para o despacho decorrente do disposto nos arts. 407, 502 ou 538 do Código de Processo Penal.

Art. 9° A gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada.

Parágrafo único. O incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Pena: reclusão, de dois a quatro anos, e multa.

Art. 11. Esta Lei entra em vigor na data de sua publicação.

Art. 12. Revogam-se as disposições em contrário.

Brasília, 24 de julho de 1996; 175º da Independência e 108º da República.

Lei de regulação de Lan House Lei 8.777 2008.

O GOVERNADOR DO ESTADO DO ESPÍRITO SANTO

Faço saber que a Assembléia Legislativa decretou e eu sanciono a seguinte Lei:

Art. 1º Todos os estabelecimentos comerciais instalados no Estado do Espírito Santo que ofertem a locação de computadores e máquinas para acesso à internet, utilização de programas e de jogos eletrônicos, abrangendo os designados como “lan houses”, “cibercafés” e “cyber offices”, entre outros, são regidos por esta Lei.

Art. 2º Os estabelecimentos de que trata esta Lei ficam obrigados a criar e manter cadastro atualizado de seus usuários, contendo:

I - nome completo;

II - data de nascimento;

III - endereço completo;

IV - telefone;

V - número de documento de identidade.

§ 1º O responsável pelo estabelecimento deverá exigir dos interessados a exibição de documento de identidade no ato de seu cadastramento e sempre que forem fazer uso de computador ou máquina.

§ 2º O estabelecimento deverá registrar a hora inicial e final de cada acesso, com a identificação do usuário e do equipamento por ele utilizado.

§ 3º Os estabelecimentos não permitirão o uso dos computadores ou máquinas por:

I - pessoas que não fornecerem os dados previstos neste artigo, ou o fizerem de forma incompleta;

II - pessoas que não portarem documento de identidade, ou se negarem a exibi-lo.

§ 4º As informações e o registro previstos neste artigo deverão ser mantidos por, no mínimo, 60 (sessenta) meses, sendo que os seus dados poderão ser armazenados em meio eletrônico com

Senha e deverão ser acondicionados em local protegido contra o acesso indevido de terceiros não autorizados.

§ 5º O fornecimento dos dados cadastrais e demais informações de que trata este artigo só poderá ser feito mediante ordem ou autorização judicial.

§ 6º Excetuadas as hipóteses previstas no § 5º, é vedada a divulgação dos dados cadastrais e demais informações de que trata este artigo.

§ 7º A divulgação ou fornecimento indevido dos dados cadastrais e demais informações fora das hipóteses previstas nesta Lei sujeitará o infrator às penalidades estabelecidas na legislação em vigor.

Art. 3º VETADO.

Art. 4º Os estabelecimentos de que trata esta Lei deverão:

I - expor em local visível lista de todos os serviços e jogos disponíveis, com um breve resumo sobre os mesmos e a respectiva classificação etária, observada a disciplina do Ministério da Justiça sobre a matéria;

II – VETADO.

III – VETADO.

IV – VETADO.

V - tomar as medidas necessárias, a fim de impedir que menores de idade utilizem contínua e ininterruptamente os equipamentos por período superior a 3 (três) horas, devendo haver um intervalo mínimo de 30 (trinta) minutos entre os períodos de uso;

VI - regular o volume dos equipamentos de forma a se adequar às características peculiares e em desenvolvimento dos menores de idade.

Art. 5º VETADO.

I - a venda e o consumo de bebidas alcoólicas;

II - a venda e o consumo de cigarros e congêneres;

III - a utilização de jogos ou a promoção de campeonatos que envolvam prêmios em dinheiro.

Art. 6º A inobservância do disposto nesta Lei sujeitará o infrator às seguintes penalidades:

I - multa, fixada entre 1.710 (mil setecentos e dez) Valores de Referência do Tesouro Estadual -VRTEs e 5.700 (cinco mil e setecentos) VRTEs, de acordo com a gravidade da infração, conforme critérios a serem definidos em regulamento;

II - em caso de reincidência, multa aplicada em dobro e cumulativamente, suspensão das atividades ou fechamento definitivo do estabelecimento, conforme a gravidade da infração.

Art. 7º O Poder Executivo regulamentará esta Lei, notadamente para especificar as atribuições inerentes à fiscalização e imposição de penalidades.

Art. 8º Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Lei de Invasão de Dispositivo Informático Lei 12.737-2012

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

“Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

"Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)

“Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Decreto de regulamentação do comercio eletrônico – decreto lei nº 7962-2013

DECRETO Nº 7.962, DE 15 DE MARÇO DE 2013

A PRESIDENTA DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, inciso IV, da Constituição, e tendo em vista o disposto na Lei no 8.078, de 11 de setembro de 1990,

DECRETA:

Art. 1º Este Decreto regulamenta a Lei no 8.078, de 11 de setembro de 1990, para dispor sobre a contratação no comércio eletrônico, abrangendo os seguintes aspectos:

I - informações claras a respeito do produto, serviço e do fornecedor;

II - atendimento facilitado ao consumidor; e

III - respeito ao direito de arrependimento.

Art. 2º Os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações:

I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;

II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;

III - características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;

IV - discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;

V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e

VI - informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta.

Art. 3º Os sítios eletrônicos ou demais meios eletrônicos utilizados para ofertas de compras coletivas ou modalidades análogas de contratação deverão conter, além das informações previstas no art. 2o, as seguintes:

I - quantidade mínima de consumidores para a efetivação do contrato;

II - prazo para utilização da oferta pelo consumidor; e

III - identificação do fornecedor responsável pelo sítio eletrônico e do fornecedor do produto ou serviço ofertado, nos termos dos incisos I e II do art. 2o.

Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá:

I - apresentar sumário do contrato antes da contratação, com as informações necessárias ao pleno exercício do direito de escolha do consumidor, enfatizadas as cláusulas que limitem direitos;

II - fornecer ferramentas eficazes ao consumidor para identificação e correção imediata de erros ocorridos nas etapas anteriores à finalização da contratação;

III - confirmar imediatamente o recebimento da aceitação da oferta;

IV - disponibilizar o contrato ao consumidor em meio que permita sua conservação e reprodução, imediatamente após a contratação;

V - manter serviço adequado e eficaz de atendimento em meio eletrônico, que possibilite ao consumidor a resolução de demandas referentes a informação, dúvida, reclamação, suspensão ou cancelamento do contrato;

VI - confirmar imediatamente o recebimento das demandas do consumidor referidas no inciso, pelo mesmo meio empregado pelo consumidor; e

VII - utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

Parágrafo único. A manifestação do fornecedor às demandas previstas no inciso V do caput será encaminhada em até cinco dias ao consumidor.

Art. 5º O fornecedor deve informar, de forma clara e ostensiva, os meios adequados e eficazes para o exercício do direito de arrependimento pelo consumidor.

§ 1º O consumidor poderá exercer seu direito de arrependimento pela mesma ferramenta utilizada para a contratação, sem prejuízo de outros meios disponibilizados.

§ 2º O exercício do direito de arrependimento implica a rescisão dos contratos acessórios, sem qualquer ônus para o consumidor.

§ 3º O exercício do direito de arrependimento será comunicado imediatamente pelo fornecedor à instituição financeira ou à administradora do cartão de crédito ou similar, para que:

I - a transação não seja lançada na fatura do consumidor; ou

II - seja efetivado o estorno do valor, caso o lançamento na fatura já tenha sido realizado.

§ 4º O fornecedor deve enviar ao consumidor confirmação imediata do recebimento da manifestação de arrependimento.

Art. 6º As contratações no comércio eletrônico deverão observar o cumprimento das condições da oferta, com a entrega dos produtos e serviços contratados, observados prazos, quantidade, qualidade e adequação.

Art. 7º A inobservância das condutas descritas neste Decreto ensejará aplicação das sanções previstas no art. 56 da Lei no 8.078, de 1990.

Art. 8º O Decreto no 5.903, de 20 de setembro de 2006, passa a vigorar com as seguintes alterações:

“Art. 10. .....

Parágrafo único. O disposto nos arts. 2º, 3º e 9º deste Decreto aplica-se às contratações no comércio eletrônico. ” (NR)

Art. 9º Este Decreto entra em vigor sessenta dias após a data de sua publicação.

Marco Civil da internet lei 12.965/2014

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I

Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no caput deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei no 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10º. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I

Da Guarda de Registros de Conexão

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.

Subseção II

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III

Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

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.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV

Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V

DISPOSIÇÕES FINAIS

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.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Lei de infiltração de Agente de polícia na Internet lei 13.441/2017

LEI Nº 13.441, DE 8 DE MAIO DE 2017.

Altera a Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), para prever a infiltração de agentes de polícia na internet com o fim de investigar crimes contra a dignidade sexual de criança e de adolescente.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º O Capítulo III do Título VI da Parte Especial da Lei nº 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), passa a vigorar acrescido da seguinte Seção V-A:

"Seção V-A

Da Infiltração de Agentes de Polícia para a Investigação de Crimes contra a Dignidade Sexual de Criança e de Adolescente"

"Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras:

I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público;

II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas;

III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.

§ 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo.

§ 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se:

I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão;

II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.

§ 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios."

"Art. 190-B. As informações da operação de infiltração serão encaminhadas diretamente ao juiz responsável pela autorização da medida, que zelará por seu sigilo.

Parágrafo único. Antes da conclusão da operação, o acesso aos autos será reservado ao juiz, ao Ministério Público e ao delegado de polícia responsável pela operação, com o objetivo de garantir o sigilo das investigações."

"Art. 190-C. Não comete crime o policial que oculta a sua identidade para, por meio da internet, colher indícios de autoria e materialidade dos crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal).

Parágrafo único. O agente policial infiltrado que deixar de observar a estrita finalidade da investigação responderá pelos excessos praticados."

"Art. 190-D.Os órgãos de registro e cadastro público poderão incluir nos bancos de dados próprios, mediante procedimento sigiloso e requisição da autoridade judicial, as informações necessárias à efetividade da identidade fictícia criada.

Parágrafo único. O procedimento sigiloso de que trata esta Seção será numerado e tombado em livro específico."

"Art. 190-E. Concluída a investigação, todos os atos eletrônicos praticados durante a operação deverão ser registrados, gravados, armazenados e encaminhados ao juiz e ao Ministério Público, juntamente com relatório circunstanciado.

Parágrafo único. Os atos eletrônicos registrados citados no **caput** deste artigo serão reunidos em autos apartados e apensados ao processo criminal juntamente com o inquérito policial, assegurando-se a preservação da identidade do agente policial infiltrado e a intimidade das crianças e dos adolescentes envolvidos."

Art. 2º Esta Lei entra em vigor na data de sua publicação.

Brasília, 8 de maio de 2017; 196º da Independência e 129º da República.

MICHEL TEMER

Osmar Serraglio

Luislinda Dias de Valois Santos

Projeto de lei que puni publicações de fotos e vídeos íntimos

PROJETO DE LEI N.º 5.555-A, DE 2013

Altera a Lei nº 11.340, de 7 de agosto de 2006 - Lei Maria da Penha criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação; tendo parecer da Comissão de Seguridade Social e Família, pela aprovação deste e dos de nº 5.822/13, 6630/13, 6.713/13, 6831/2013, e 7.377/14, apensados, com substitutivo (relator: DEP. DR. ROSINHA).

DESPACHO: ÀS COMISSÕES DE:

SEGURIDADE SOCIAL E FAMÍLIA E CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (MÉRITO E ART. 54,RICD)

APRECIAÇÃO:

Proposição Sujeita à Apreciação do Plenário

S U M Á R I O

I – Projeto inicial

II – Projetos apensados: 5.822/13, 6.630/13, 6.713/13, 6.831/13 e 7.377/14.

III – Na Comissão de Seguridade Social e Família:

- Parecer do Relator
- Substitutivo oferecido pelo Relator
- Parecer da Comissão
- Substitutivo adotado pela Comissão

AVULSO NÃO PUBLICADO. PROPOSIÇÃO DE PLENÁRIO.

Coordenação de Comissões Permanentes - DECOM - P_4556

CONFERE COM O ORIGINAL AUTENTICADO

PL-5555-A/2013

O Congresso Nacional decreta:

Art. 1º Esta Lei altera a Lei nº 11.340, de 7 de agosto de 2006 – Lei Maria da Penha – criando mecanismos para o combate a condutas ofensivas contra a mulher na Internet ou em outros meios de propagação da informação.

Art. 2º O artigo 3º da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar com a seguinte redação: “Art. 3º Serão asseguradas às mulheres as condições para o exercício efetivo dos direitos à vida, à segurança, à saúde, à alimentação, à educação, à cultura, à comunicação, à moradia, ao acesso à justiça, ao esporte, ao lazer, ao trabalho, à cidadania, à liberdade, à dignidade, ao respeito e à convivência familiar e comunitária.” (NR)

Art. 3º O artigo 7º da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar acrescido do inciso VI, com a seguinte redação:

“Art. 7º.....

VI – violação da sua intimidade, entendida como a divulgação por meio da Internet, ou em qualquer outro meio de propagação da informação, sem o seu expresso consentimento, de imagens, informações, dados pessoais, vídeos, áudios, montagens ou fotocomposições da mulher, obtidos no âmbito de relações domésticas, de coabitação ou de hospitalidade.”(NR)

Art. 4º O artigo 22 da Lei nº 11.340, de 7 de agosto de 2006, passa a vigorar acrescido do parágrafo 5º, com a seguinte redação:

“Art.22.....

§5º Na hipótese de aplicação do inciso VI do artigo 7º desta Lei, o juiz ordenará ao provedor de serviço de e-mail, perfil de rede social de hospedagem de site, de hospedagem de blog, de telefonia móvel ou qualquer outro prestador do serviço de propagação de informação, que remova, no prazo de 24 (vinte e quatro) horas, o conteúdo que viola a intimidade da mulher.(NR)”

Art.5º Esta Lei entra em vigor na data de sua publicação.

Estatuto da criança e do adolescente (ECA)

LEI Nº 11.829, DE 25 DE NOVEMBRO DE 2008.

O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Os arts. 240 e 241 da Lei no 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação:

“Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:

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

§ 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.

§ 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:

I – no exercício de cargo ou função pública ou a pretexto de exercê-la;

II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou

III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.” (NR)

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

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

Art. 2º A Lei no 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:

"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 pornográfica envolvendo criança ou adolescente:

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

§ 1º Nas mesmas penas incorre 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 cena de sexo explícito ou pornográfica 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, 241-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 funcionários responsáveis 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.

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 visual:

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 a se exibir de forma pornográfica ou sexualmente explícita.

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”.

Art. 3º Esta Lei entra em vigor na data de sua publicação.

Brasília, 25 de novembro de 2008; 187º da Independência e 120º da República.

LUIZ INÁCIO LULA DA SILVA

LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

Art. 2º (VETADO)

Art. 3º (VETADO)

Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 5º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20. .....

§ 3º .....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

Paulo Bernardo Silva

Maria do Rosário Nunes

Este texto não substitui o publicado no DOU de 3.12.2012

17 REFERÊNCIAS

ANTÔNIO, Roberto Darós Malaquias. **Crimes cibernéticos e prova: a investigação criminal em busca da verdade.** Curitiba: Juruá, 2012, p. 60.

AMIN, Andréa Rodrigues et al. **Curso de Direito da Criança e do Adolescente – Aspectos teóricos e práticos.** Rio de Janeiro: Lumen Juris, 2006.

BRASIL. Lei nº 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/l8069.htm>. Acesso em: 01. mar. 2017.

Blog magic web desing Combate a crimes virtuais no Brasil. Disponível em: < http://www.magicwebdesign.com.br/blog/internet/combate-crimes-virtuais-brasil/ > Acesso em: 26 jul 2017.

Blasting News. Jovem de MG cumpriu a última tarefa do jogo da Baleia Azul. Ele se matou. Disponível em: < http://br.blastingnews.com/brasil/2017/04/jovem-de-mg-cumpriu-a-ultima-tarefa-do-jogo-da-baleia-azul-ele-se-matou-001625551.html?sbdht=_pM1QUzk3wscaKeYjyjDap0rH_0Q-vyaG_E0ruJzl3B0HSmzsFUpZfA2_ >. Acesso em: 02 jul 2017.

BRASIL. Constituição da República Federativa do Brasil. 05 de outubro de 1988. Disponível em: < https://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>. Acesso em: 14 jul 2017.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 25 ago 2017.

BRASIL. Lei nº 8069 DE 13 DE Julho de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L8069.htm Acesso em: 25 ago 2017.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm >. Acesso em: 25 ago 2017.

BRASIL. Decreto Lei nº L ei nº 11.829, de 25 de novembro de 2008. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm >. Acesso em: 25 ago. 2017.

BRASIL. Decreto Lei nº 7.962, de 15 de março de 2013. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7962.htm >. Acesso em: 25 ago. 2017.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípio, garantias, direito e deveres para o uso da Internet no Brasil Disponível em: <

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 25 ago. 2017.

BRASIL. Lei nº 8.777 de 2007 Disponível em: < http://www.al.es.gov.br/antigo_portal_ales/images/leis/html/LO8777.html >. Acesso em: 25 ago. 2017.

BRASIL. Lei nº 9.296, de 24 de Julho de 1996. Regulamenta o inciso XII parte final, do art 5º da Constituição Federal. Lei da Interceptação Telefônica. Brasília, Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9296.htm >. Acesso em: 25 ago. 2017.

BRASIL. PL 2793/2011. Disponível em: < http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011 >. Acesso em: 25 ago. 2017.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011.p.90.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 12, 5 maio 1997. Disponível em: <https://jus.com.br/artigos/1826>. Acesso em: 31 jul.2017.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. In: Âmbito Jurídico, Rio Grande, XV, n. 99, abr 2012. Disponível em: < http://www.ambitojuridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529. >. Acesso em ago 2017.

CASTRO, Dione Silva de. Do crime de violação de correspondência e da invasão de dispositivo informático. Disponível em: < https://dionecastro.jusbrasil.com.br/artigos/341812431/do-crime-de-violacao-de-correspondencia-e-da-invasao-de-dispositivo-informatico >. Acesso em: 26 jul. 2017.

CICERA. Crimes virtuais: conceito e seus tipos Disponível em: < https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus-tipos. >. Acesso em: 07 jul 2017.

Câmara dos Deputados. DTAQ. 2013. Disponível em: < http://www.camara.gov.br/sileg/integras/1095079.pdf >. Acesso em: 20 ago 2017.

ELIAS, Paulo Sá. **A tecnologia e o Direito no século XXI: nova abordagem**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7, n. 53, 1 jan. 2002. Disponível em: <https://jus.com.br/artigos/2547>. Acesso em: 31 jul. 2017.

Estado de Alagoas. Conselho da criança e do adolescente. Disponível em: < http://www.conselhodacrianca.al.gov.br/sala-de-imprensa/noticias/2013/marco/o-que-e-o-eca >. Acesso em: 25 ago. 2017.

CAPEZ, Fernando **Curso de direito penal parte especial** edição 17º, p. 117. Ano 2017.

G1.com. Entenda o caso de Edward Snowden, que revelou espionagem dos EUA. Disponível em: < http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html (reportagem do marco civil). Acesso em: 05 jul 2017.

Gazeta do povo Como a Rússia deu origem à Baleia Azul, jogo de suicídio que preocupa o Brasil. Disponível em: < http://www.gazetadopovo.com.br/ideias/como-a-russia-deu-origem-a-baleia-azul-jogo-de-suicidio-que-preocupa-o-brasil-944jc99a8hw9d37fosnfhjac4 >. Acesso em: 02 jul. 2017.

G1.com. #LikES: Já ouviu falar no Sarahah? Saiba que ele pode virar caso de polícia. Disponível em: < http://gshow.globo.com/TV-Gazeta-ES/Em-Movimento/noticia/likes-ja-ouviu-falar-no-sarahah-saiba-que-ele-pode-virar-caso-de-policia.ghtml >. Acesso em: 18 ago 2017.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.49.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. São Paulo: Editora Juarez de Oliveira, 2004. p.51.

Jornal de Brasília. Prostituição corre livre na internet. Disponível em: < http://www.jornaldebrasilia.com.br/cidades/prostituicao-corre-livre-na-internet/ >. Acesso em: 25 ago. 2017.

Jusbrasil. Justiça usa Código Penal para combater crime virtual: disponível em: http://stj.jusbrasil.com.br/noticias/234770/justiça-usa-código-penal-para-combater-crime-virtual >. Acesso em: 07 jul 2017.

Jusbrasil. TJ-CE - Habeas Corpus : HC 06282641420158060000 CE 0628264-14.2015.8.06.0000.Disponívelem:<https://tjce.jusbrasil.com.br/jurisprudencia/305965611/habeas-corpus-hc-06282641420158060000-ce-0628264-1420158060000 >. Acesso em: 25 ago 2017.

LIMA, Paulo Marcos Ferreira. Crimes de Computador e Segurança Computacional 2 ed. Campinas/SP: Millennium, 2007, p.71.

MAGGIO, Vicente de Paula Rodrigues. Novo crime: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: < https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a >. Acesso em: 26 jul 2017.

Metrópoles. Divulgar nudes sem autorização é crime. Disponível em: < http://www.metropoles.com/vida-e-estilo/comportamento/vazar-nudes-sem-autorizacao-e-crime >. Acesso em: 25 ago 2017

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.91.

Revista Consultor Jurídico, 26 de dezembro de 2016. O Marco Civil da Internet se consolida nos tribunais brasileiros http://www.conjur.com.br/2016-dez-26/retrospectiva-2016-marco-civil-internet-consolida-tribunais >. Acesso em: 05 jul 2017.

Último segundo ig. Preso, criador do jogo de suicídio Baleia Azul fala em 'limpeza da sociedade'. Disponível em: < http://ultimosegundo.ig.com.br/mundo/2017-05-10/baleia-azul.html >. Acesso em: 02 jul 2017.

SOUKI, Hassan Magid de Castro. O uso da internet e os crimes cibernéticos. Disponível em: < http://www.migalhas.com.br/dePeso/16,MI246765,81042-O+uso+da+internet+e+os+crimes+ciberneticos >. Acesso em: 17 ago 2017.

VINICIUS, Higor Nogueira Jorge. WENDT, Emerson. **Crimes cibernéticos: ameaças e procedimentos de investigação**. 2 ed. Rio de Janeiro: Brasport, 2013. P. 12.

Veja Abril Falso Justin Bieber é acusado de 931 crimes de pedofilia. Disponível em: < http://veja.abril.com.br/mundo/falso-justin-bieber-e-acusado-de-931-crimes-de-pedofilia/ >. Acesso em: 21 mar. 2017.

ZH Vida e Estilo. Projeto de lei pune vazamento de fotos íntimas. Disponível em: < http://zh.clicrbs.com.br/rs/vida-e-estilo/noticia/2017/02/projeto-de-lei-pune-vazamento-de-fotos-intimas-9728371.html >. Acesso em: 25 ago 2017.