



FACULDADES DOCTUM DE CARATINGA

MIRIAM FORTUNATO MARTINS

CRIMES VIRTUAIS – UMA ANÁLISE DA LEI 12.737/2012

Caratinga – MG

2019

CRIMES VIRTUAIS – UMA ANÁLISE DA LEI 12.737/2012

Monografia apresentada ao Curso de Direito das Faculdades Doctum de Caratinga, como exigência parcial à obtenção do grau de Bacharel em Direito.
Áreas de concentração: Direito Penal e Direito Constitucional.
Orientador: Prof. Luiz Eduardo Moura Gomes.


**Caratinga - MG
2019**

TERMO DE APROVAÇÃO

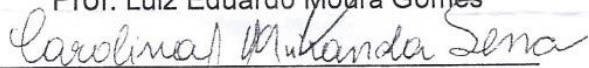
Trabalho de Conclusão de Curso **Crimes Virtuais - Uma análise da lei 12.737/2012**, elaborado **Miriam Fortunato Martins** a foi aprovado por todos os membros da Banca Examinadora e aceita pelo curso de Direito da FACULDADES DOCTUM DE CARATINGA, como requisito parcial da obtenção do título de

BACHAREL EM DIREITO.

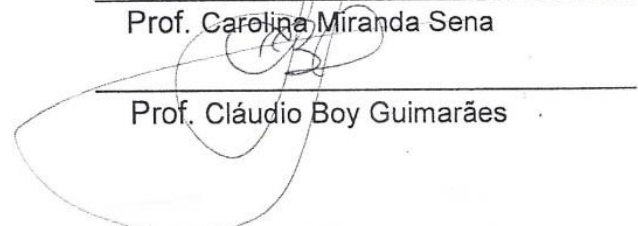
Caratinga 05 de DEZEMBRO 20 19



Prof. Luiz Eduardo Moura Gomes



Prof. Carolina Miranda Sena



Prof. Cláudio Boy Guimarães

DEDICATÓRIA

Dedico esta monografia primeiramente a Deus, que sempre estará de olho em nós, aos meus pais, e irmãos que sempre estiveram presentes na minha vida traçando esse caminho para minha formação tanto pessoal como profissional.

E na vida através de dificuldades e obstáculos traçados, de superações, desses conhecimentos adquiridos, com esforços e sacrifícios que hoje damos mais um passo, e somamos mais um ponto para conquistarmos nossos objetivos durante esta jornada.

“Família é um grupo de pessoas, cheios de defeitos, que Deus reúne para que convivam com as diferenças e desenvolvam a tolerância, a benevolência, a caridade, o perdão, o respeito, a gratidão, a paciência, direito e dever, limites, enfim, que aprendam a AMAR: fazendo ao outro o que quer que o outro lhe faça. Sem exigir deles a perfeição que ainda não temos. Nós não nascemos onde merecemos, mas onde necessitamos evoluir. ” (Papa São Francisco)

AGRADECIMENTOS

Agradeço primeiramente a Deus.

Agradeço aos amigos que tinha e aos que conheci durante essa jornada, que me ajudaram diretamente ou indiretamente para a conclusão.

Agradeço meus pais, Luiz Antônio e Mariza, onde partiu minha inspiração para a vida acadêmica, onde sempre me incentivaram e ajudaram nas dificuldades ao longo desta caminhada no curso de Direito.

Agradeço aos meus Irmãos Mário e Mateus, que sempre souberam as palavras certas a se usar nas oportunidades que tiveram e apoio não deixando as dificuldades me derrubarem.

Agradeço aos meus amigos e colegas da faculdade que sempre torceram por mim.

Agradeço aos professores que sempre ajudaram no aprendizado e nas dificuldades, em especial ao meu orientador e Professor Luiz Eduardo Moura Gomes.

Enfim a todos os que acreditaram e me apoiaram em mais essa vitória!

RESUMO

A civilização, no início século XXI, tem sido constantemente impactada por novidades tecnológicas que emergem em diversos campos da ciência numa velocidade inédita na História. Nenhuma, porém, causou tão profunda mudança no comportamento humano como a internet, rede internacional de comunicação desenvolvida a partir do último quarto do século passado. Meio de comunicação originalmente criado para fins militares e acadêmicos, a internet foi internacionalmente popularizada em meados dos anos 90, quando passou a ser utilizada principalmente para navegação (*world wide web*), correspondência (*e-mail*) e conversas (*chats*) eletrônicas. De tempos em tempos, e cada vez com maior rapidez, a internet apresenta novos serviços e atividades, o que recentemente desencadeou a adoção de um novo conceito para definir a sua atual fase – Web 2.0. A expressão refere-se à segunda geração de serviços e aplicativos da Web e aos recursos, tecnologias e conceitos que permitem um maior grau de interatividade e colaboração dos usuários na utilização da internet. A tecnologia, *lato sensu*, pode ser usada para fins lícitos ou ilícitos, gerar benefícios e malefícios, riquezas para uns e falência para outros. Por um lado, serve para melhorar a comunicação, aumentar a qualidade de vida, o conforto, o entretenimento, a saúde; por outro, pode ser usada para potencializar atividades criminosas como a pedofilia, o estelionato, os abusos ao meio ambiente, a pirataria, a experiência científica sem análise da nocividade, em afronta a princípios fundamentais, como o da Dignidade da Pessoa Humana, previsto no artigo 1º, inciso III, da Constituição da República Federativa do Brasil. O objetivo deste trabalho é qual a forma de controle no ordenamento jurídico brasileiro para evitar o uso inadequado da Internet. A metodologia utilizada foi a pesquisa bibliográfica, entre livros e artigos publicados sobre o assunto.

Palavras-chave: Crimes Virtuais, Internet, Direitos Fundamentais

SUMÁRIO

INTRODUÇÃO	9
CAPÍTULO I	11
1 - A INTERNET E SUAS VANTAGENS E SEUS RISCOS.....	11
1.1 - Meios Utilizados por Atacantes para Ter Acesso ao Computador do Usuário	12
1.2 - Principais Ameaças.....	14
1.3 - Crimes Virtuais	16
CAPÍTULO II	21
2 - PRINCÍPIOS E GARANTIAS DO MARCO CIVIL	21
2.1 - Fundamentos Jurídicos do Marco Civil.....	25
2.2 - Inclusão Social e Digital	30
2.3 - Direitos dos Usuários de Internet.....	31
CAPÍTULO III.....	34
3 - CRIMES CIBERNÉTICOS E A FRAGILIDADE DA LEI 12.737/12.....	34
3.1- Dos Crimes Cibernéticos.....	35
3.2- Considerações Sobre Crime.....	35
3.2.1- Do Uso Da Analogia.....	36
3.3- Algumas Considerações Sobre a Lei 12.737/12 e Exposição De Seus Motivos.....	38
3.4- Análise Da Matéria Tratada Na Lei 12.737/12.....	40
3.5 – Da Fragilidade Da Lei 12.737/12.....	43
CONSIDERAÇÕES FINAIS	47
REFERÊNCIAS	49

INTRODUÇÃO

Com a globalização e a evolução tecnológica, a troca de informações passa a ser feita em tempo real, fundando a Era Digital e gerando novos tipos de preocupações. Com o advento da Internet e a realidade da era digital e *on-line*, indispensável e a adequação do Direito, que necessita afiar seus instrumentos e lançar luzes sobre as novas relações sociais que se delineiam, pois, juntamente com a evolução tecnológica, inaugura-se a era de crimes virtuais.

O Direito da Sociedade da Informação, nova vertente do Direito que se relaciona intimamente com a era de evolução tecnológica que ora se apresenta, tem relação estreita com os fenômenos e processos de pesquisas tecnológicas. Nesse patamar estão os crimes praticados por meio do uso de sofisticadas tecnologias. Estamos todos conectados e a informação se propaga em alta velocidade.

O presente trabalho acadêmico terá como marco teórico a base de raciocínio do Professor Rogério Greco, onde este discorre em seu livro Código Penal Comentado de 2012:

“Entendemos que essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto pelo art. 154-A do diploma repressivo quando, também, mesmo indevidamente, ingresse em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois que inexistente”.

Crimes virtuais acontecem com grande frequência. Portanto, a segurança da Informação é hoje um problema sério e contínuo enfrentado por centenas de países. Atualmente, criminosos utilizam ferramentas dotadas de alta tecnologia com poder imensurável de ação, seja para destruir dados, seja para capturar informações sigilosas, extorquindo autoridades e governos.

A informação e a disponibilidade da informação passam a ter um grande valor para empresas e governos. Cresce a cada dia a necessidade de proteção do capital intelectual e proteção da capacidade de gerar e receber informações.

Nas empresas, nasce o conceito de que o capital humano deve ser mais protegido que outrora, uma vez que uma mensagem eletrônica mal-

intencionada pode comprometer a reputação de governos, Estados, empresas ou mercados. Nessa nova realidade, nasce uma nova cultura, a de que as políticas de segurança da informação cada vez mais são objeto de projetos críticos de sucesso de empresas privadas e de entidades públicas.

A presente pesquisa científica pretende investigar algumas das múltiplas faces dos crimes cibernéticos e por sua vez os crimes praticados por meio de avançadas ferramentas tecnológicas e seus reflexos no mundo Jurídico com a fonte de preocupação para a implantação de novas ferramentas de controle eletrônico do governo no Brasil.

No primeiro capítulo será abordado sobre os benefícios que a era digital nos trouxe, assim como os seus riscos e como somos atacados por *hackers*, e os meios mais utilizados para invadir nossa privacidade digital.

No segundo capítulo será abordado marco civil, que visa regular o uso da internet no Brasil, assim como se tenta controlar o seu uso pela população.

No terceiro capítulo será abordado sobre crimes cibernéticos e a fragilidade da Lei 12.737/12.

Este estudo se entende de grande relevância para a comunidade acadêmica, pois pretende-se, sem que se esgote o assunto, dar uma contribuição para a situação alarmante da invasão de nossa privacidade.

O Estado deve atuar de forma que não existam lacunas em relação à aplicação de suas Leis, em especial, as Leis que definem crimes devem ser precisas, deixando claro a conduta que objetivam punir. Em razão do princípio da legalidade não é admitido no Ordenamento Jurídico a existência de leis vagas e imprecisas, ou seja, Leis estas que não deixam perfeitamente delimitado o comportamento a ser incriminado e punido, podendo a ser a estes elencado o nome de “tipos penais abertos”.

CAPÍTULO I

1 - A INTERNET: SUAS VANTAGENS E SEUS RISCOS

Ao estudar a doutrina de C., a internet é uma grande praça pública, o maior espaço coletivo do planeta. Estima-se que no final de 2013 cerca de 2,7 bilhões de pessoas em todo o mundo estarão conectadas. No Brasil a internet está atingindo um número crescente de usuários; somos 105 milhões de internautas que estão cada vez mais conectados e passando mais tempo *on-line*.

A internet é um conjunto de redes de comunicações em escala mundial e dispõe de milhões de computadores interligados pelo protocolo de comunicação TCP/IP, que permite o acesso a informações e todo tipo de transferência de dados. A Internet carrega uma ampla variedade de recursos e serviços num espaço virtual também chamado de ciberespaço, daí que, como no mundo real, a segurança digital é um terreno de ferrenha disputa entre defensores e agressores. (CASSANTI, 2014, p. 133)¹

O entendimento de C., complementa que a partir do segundo semestre do ano de 2011 acompanhamos um aumento muito expressivo dos chamados dispositivos móveis como celulares, *smartphones* e *tablets*. Com isso, os ataques virtuais que antes eram restritos aos computadores estão migrando para as plataformas móveis. Assim como os computadores, os dispositivos móveis podem ser usados para a propagação de códigos maliciosos, furto de dados, envio de *spam*, além de poder fazer parte de *botnets* e serem usados para disparar ataques na Internet.

O acesso à internet, *e-mails*, aplicativos e principalmente às redes sociais a partir de qualquer lugar são algumas das facilidades oferecidas por esses dispositivos.

Para A.², algumas características próprias que os dispositivos móveis possuem os tornam mais atraentes para atacantes e pessoas mal-intencionadas como:

¹ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p.133.

² ASCENÇÃO, José de Oliveira. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.p. 133.

- ✓ Grande quantidade de informações pessoais armazenadas.
- ✓ Maior possibilidade de perda e furto.
- ✓ Grande quantidade de aplicações desenvolvidas por terceiros.
- ✓ Rapidez de substituição dos modelos.

De forma geral, os cuidados que você deve tomar para proteger seus dispositivos móveis são os mesmos a serem tomados com seu computador pessoal, como mantê-los sempre atualizados e utilizar mecanismos de segurança.

1.1 - Meios Utilizados por Atacantes para Ter Acesso ao Computador do Usuário

Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais se quem pretender vencê-lo primeiramente não puder entendê-lo.

Muitos não sabem, mas para o usuário ser atacado, ele precisa permitir que isso aconteça de forma direta ou indireta. Na forma indireta, o atacante, para "entrar" na máquina, explora as vulnerabilidades, tanto por falhas nos softwares ou por configurações incorretas do computador, ou de segurança proporcionadas pelo *firewall*. Da forma direta, o atacante se utiliza de um dos meios listados a seguir para implantar um programa malicioso (*malware*) no computador do usuário e assim prosseguir com o ataque. (MARQUES, 2012, p. 98)³

M. afirma que atualmente, o *e-mail* tornou-se um meio de comunicação indispensável, mas, por outro lado, ainda é um dos meios mais eficazes para que um atacante invada um computador. *Spam*, vírus, golpes de roubo de identidade e e-mails fraudulentos são apenas algumas das ameaças. O usuário recebe um e-mail fazendo despertar sua curiosidade e acaba clicando em um link, permitindo assim que o atacante alcance o seu objetivo.

Ainda sobre o uso do *e-mail*, M., afirma que:

São programas para enviar e receber mensagens simultaneamente. A comunicação é feita em tempo real por meio de textos, voz ou vídeo. As conversas podem ser feitas entre duas ou mais pessoas em ambiente privado.

³ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012, p. 98.

Nos ensinamento de Schaff⁴, pondera que hoje muitos são os programas que executam esta tarefa, a exemplo do *Skype*, *Yahoo Messenger*, *Google Talk*, dentre outros. Apesar de alguns detalhes variarem de um programa para outro, os passos básicos são os mesmos para qualquer utilitário de mensagens instantâneas disponíveis. Em programas de mensagens instantâneas o mais comum é o atacante mandar um link através de uma pessoa conhecida. Se o usuário clica, a ameaça se instala no computador. Outro problema é que estes programas abrem portas que permitem ao atacante capturar o IP da máquina.

Assim define níveis de redes sociais P.:

“Alguns dos níveis da rede social mais conhecido são, sem dúvidas, os sites de relacionamentos (*Facebook*, *Orkut*, *Myspace*, *Twitter* e muitos outros). Estes sites facilitam o encontro de pessoas que por algum motivo estavam afastadas e permitem fazer novas amizades por comunidades semelhantes. Mas o preço para quem se insere nessas redes é a sua privacidade, que estará aberta a todos os usuários da internet, ou seja, todos passam a obter informações sobre rotina, identidades e estilos de vidas dos participantes daquela comunidade.”⁵

Não existem ferramentas de segurança voltadas para proteger as pessoas de si mesmas; sabendo disso, as redes sociais estão sempre na mira dos atacantes, pois é muito fácil enganar usuários desavisados.

No entender de Cassanti, uma recente pesquisa realizada pela *Kaspersky Lab* apontou que 21% dos links maliciosos presentes na internet estão hospedados em redes sociais, contra 14% que estão disponibilizados em sites de conteúdo adulto. Segundo o estudo, sites como *Facebook*, *Twitter* e *Google+* tornaram-se uma arma em potencial para os atacantes, pois, quanto mais popular, maior a possibilidade da criação de links maliciosos para serem propagados pela rede:

“O vencedor de maior disseminação de malware é o *YouTube*, que abriga atualmente 31 % dos links maliciosos. Os serviços de busca, como o *Google*, ficam em segundo lugar, com 22%, onde é realizada manipulação de resultados para o redirecionamento a links maliciosos”.⁶

⁴ SCHAFF, Adam. **A Sociedade Informática**. Traduzido por Carlos Eduardo J. Machado 4ª ed. São Paulo: Brasiliense, 1995, p. 178.

⁵ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000, p. 89.

⁶ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000, p. 87.

Esses programas servem para compartilhar e localizar arquivos. Com eles você pode encontrar e fazer *download* de músicas MP3, vídeos AVI, MPEG e muitos outros formatos de arquivos, até mesmo programas. Entre os mais utilizados estão: o *Ares*, *LimeWire*, *eMule* etc. e todos disponibilizam milhares de arquivos, mas nem todos são confiáveis.

Usam técnicas de redirecionamento em que eventualmente o usuário pode ser direcionado para um site falso, idêntico ao original, que lhe solicitará senha. Caso o usuário não desconfie, além do site lhe roubar alguma senha, poderá instalar algum tipo de programa malicioso.

Dessa forma, é ensinado que o formato PDF hoje em dia é um dos maiores vetores de ataques para instalações de códigos maliciosos, isso porque ele permite a execução de *Javascript* e *flash object* embarcados no arquivo. Podem carregar *exploits* para o Adobe Reader e, quando a pessoa abre o arquivo, se instala o trojan. A dica de segurança para o PDF é utilizar leitores alternativos ao *Adobe Reader*, como o *Foxit*, por exemplo.

1.2 - Principais Ameaças

No entendimento de S.⁴: “um computador é vulnerável quando este apresenta varias deficiências de segurança. Antivírus desatualizado, sistemas operacionais piratas (que não podem receber atualizações), *firewall* desativado ou configurações incorretas da rede e ainda falhas nos *softwares*. Os atacantes exploram essas vulnerabilidades, resultando em possíveis ataques e danos para o computador ou seus dados pessoais” .

No entendimento de P.⁶, “o termo *malware* é a contração de "malicious software" (programa malicioso) e identifica qualquer programa desenvolvido com o propósito de causar dano a um computador, sistema ou redes de computadores. É um dos dois tipos de intrusos que podem invadir o seu computador (o outro é o próprio atacante). Os mais comuns são os vírus, *worms* e cavalos de troia. Geralmente se utilizam de ferramentas de comunicação conhecidas para se espalharem - como, por exemplo, *worms* enviados por *e-mail* e mensagens instantâneas, cavalos de troia provenientes de websites e arquivos infectados com vírus obtidos por download de conexões ponto-a-ponto. O *malware* também tenta explorar as vulnerabilidades existentes nos sistemas, tornando sua entrada discreta e fácil”.

Os vírus são pequenos programas capazes de produzir cópias de si mesmo, porém não podem se auto executarem; para começar a agir, precisam

que alguém ou algo os execute.

M. ensina, “que os vírus não podem se auto executar para burlar esta deficiência; é preciso que um programa previamente infectado seja executado”⁷. Assim, se um programa contaminado for salvo em um HD, isso não vai proporcionar o ataque do vírus; enquanto o evento que ativa o vírus não for acionado pelo usuário, o vírus ficará "adormecido". Outro mito que deve ser desfeito é de que os vírus podem danificar o *hardware* do computador. Os vírus são softwares, portanto não há como eles queimarem ou quebrarem dispositivos do computador; o que pode ocorrer é de um vírus contaminar o BIOS de uma placa-mãe fazendo-a parar de funcionar, dando a impressão de que foi quebrada, mas existem laboratórios que recuperam o BIOS eliminando o vírus nele contido.

1.3 - Crimes Virtuais

No ensinamento de A., “os crimes virtuais não são praticados apenas por atacantes com conhecimento sofisticado de informática”⁸. Crimes cometidos por e-mails como calúnia (acusar alguém de um crime que não cometeu), agressão e desrespeito por motivo de cor, raça, etnia ou religião são cada vez mais frequentes entre os usuários, que utilizam na maioria das vezes redes sociais como *Facebook*, *Twitter*, *YouTube* ou os *blogs* para práticas desses delitos. Muitas vezes os autores acreditam que suas ações ficarão impunes.

No entendimento de M., o que incentiva os crimes virtuais:

“O maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis, mas é importante saber que quando o computador é uma ferramenta para prática dos delitos, suscita a possibilidade de se amoldar aos tipos penais já existentes. Por exemplo, a calúnia pode ser praticada tanto em um jornal quanto na internet: é o mesmo crime, mudando apenas o meio de sua efetivação, potencializando a sua comunicação. Neste caso, as penas aplicadas são as mesmas, independentemente do meio utilizado para a prática do crime”⁹.

A lista de crimes cometidos por meio eletrônico é extensa. Na grande maioria dos casos é possível adaptar os crimes virtuais à legislação vigente. Ainda, de acordo com o que pensa A., o Judiciário vem coibindo diariamente a

⁷ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.p. 276.

⁸ ASCENÇÃO, José de Oliveira. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.p. 137.

⁹ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.p. 291.

sensação de impunidade que reina no ambiente virtual e combatendo a criminalidade cibernética com a aplicação do Código Penal, do Código Civil e de legislações específicas como a Lei n. 9.296/96 - que trata das interceptações de comunicação em sistemas de telefonia, informática e telemática - e a Lei n. 9.609/98 - que dispõe sobre a proteção da propriedade intelectual de programas de computador.

No estudo de P., para o Judiciário, 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizarem crimes comuns praticados através da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, a exemplo da distribuição de vírus eletrônico e dos ataques DDoS.

Neste tipo de contravenção criminosos usam dados pessoais alheios para aplicarem golpes na emissão de cartões de crédito, abertura de contas correntes, abertura de empresas, fazer empréstimos e compra de bens.

E complementa P., “que o furto de identidade não é novidade”¹⁰. Em sua doutrina C., ensina que:

“A Serasa Experian registrou 2,14 milhões de tentativas de fraudes contra o consumidor em 2012; um aumento de 10% se comparados aos 1,96 milhão de 2011. Só de janeiro a maio de 2013, foram registradas 837.641 tentativas de fraude. Segundo a empresa, o resultado mostrou que a cada quinze segundos um consumidor brasileiro foi vítima de tentativa de furto de identidade. Isso acontece porque é comum as pessoas fornecerem seus dados pessoais em cadastros na internet sem verificar a idoneidade e a segurança dos sites. Outro fator impulsionador desse tipo de ação é a popularização das mídias sociais.”¹¹

O *Phishing* é um dos meios mais utilizados pelos atacantes para obter o maior número de informações possível do usuário, pois quanto mais dados o golpista tem disponível, mais convincente ele será quando estiver se passando pela vítima.

¹⁰ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 99.

¹¹ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 234.

“Enquanto escrevia este livro recebi um *Phishing* na minha caixa postal onde o atacante tenta despertar minha curiosidade. O remetente era uma pessoa que realmente estava na minha lista de contatos, o que me leva a crer que sua máquina está contaminada e talvez ele nem saiba disso. A mensagem fraudulenta dizia que ele estava precisando de dinheiro e pedia para eu visualizar a cópia de um cheque que eu teria passado para ele”.¹²

No entendimento de B. J.,¹³ “ao clicar na imagem do cheque é transferido para o meu computador um trojan que, além de começar a espionar minhas ações até conseguir obter alguma vantagem, ainda usará minha lista de contatos para se auto enviar, aumentando assim o número de vítimas”.

Complementa B. J.,¹⁴ “que consiste em produzir, publicar, vender, adquirir e armazenar pornografia infantil pela rede mundial de computadores, por meio das páginas da *web*, *e-mail*, *newsgroups*, salas de bate-papo (*chat*), ou qualquer outra forma. Compreende, ainda, o uso da internet com a finalidade de aliciar crianças ou adolescentes para realizarem atividades sexuais ou para se explorem de forma pornográfica”.

Complementa P.¹⁵, “que para conquistar a confiança das crianças e dos adolescentes os criminosos utilizam perfis falsos e uma linguagem diferenciada, com intuito de programar encontros virtuais e presenciais que viabilizam a prática de atos de violência sexual”.

Em muitos casos oferecem oportunidades imperdíveis, presentes ou até mesmo dinheiro para convencer a vítima a marcar um encontro ou pedem para que se façam fotos e vídeos pornográficos.

No entendimento de C.,¹⁶ um estudo realizado em outubro de 2012 pelo CGI (Comitê Gestor da Internet) apontou ser preocupante a popularização das redes entre crianças e adolescentes. Os números indicam que 2,70% dos jovens entre 9 e 16 anos têm seu próprio perfil em algum site

¹² MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012. **responsabilidade civil**. São Paulo: Atlas, 2000.p. 268.

¹³ BARRETO JUNIOR, Irineu Francisco. **A relevância do conceito sociedade da informação para a pesquisa jurídica**. In: PAESANI, Liliana Minardi. **Direito na sociedade da informação**. São Paulo: Atlas, 2007, p. 276.

¹⁴ BARRETO JUNIOR, Irineu Francisco. **A relevância do conceito sociedade da informação para a pesquisa jurídica**. In: PAESANI, Liliana Minardi. **Direito na sociedade da informação**. São Paulo: Atlas, 2007, p. 276.

¹⁵ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 268.

¹⁶ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 238.

de relacionamento e desses 13% postaram os endereços de casa na internet e divulgaram seus telefones.

O mesmo estudo mostrou que as crianças não sentem pudor em publicar informações privadas e fotos dentro das redes sociais: 86% dos entrevistados possuem ao menos uma foto de seu rosto publicada, 69% já divulgaram seu sobrenome e 28% informaram a escola em que estudam.

Continua C.¹⁷, que 23% dos jovens já tiveram contato com desconhecidos por meio da Internet ou já tiveram encontro real.

Como exemplo C.¹⁸ cita o que aconteceu com uma estudante de 14 anos em São Paulo, em caso mostrado pela mídia em agosto de 2012. Após contato feito através de uma sala de bate-papo, a adolescente foi convencida por um casal a participar de uma sessão de sadomasoquismo, onde foram feitas algumas fotos e posteriormente divulgadas na internet. Em troca, a estudante ganhou um espartilho.

O casal foi preso logo depois que o pai da menina percebeu mudanças de comportamento na filha e passou a vigiá-la, instalando um software espião no notebook da adolescente. Ele informou à polícia, que prosseguiu com as investigações.

Em sua ótica M., cita que:

“apesar de pouco conhecida pelo público, a Polícia Civil de São Paulo criou em novembro de 2011 a 4ª Delegacia de Repressão à Pedofilia, única delegacia no Brasil especializada nesse tipo de crime. Investigadores passando-se por crianças conseguem se infiltrar em redes de pedofilia que agem em diversas redes sociais. O trabalho, pioneiro, resultou em um cadastro e um banco de dados, que contêm dados como foto, nome, cor de pele, idade e histórico de crimes dos pedófilos, permitindo rastrear muitos abusadores de crianças. Segundo a delegacia, 40% desses criminosos têm entre 18 e 40 anos, 25% estão acima dos 40 e o restante é menor de idade”.¹⁹

¹⁷ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 238.

¹⁸ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 238-239.

¹⁹ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.p. 287.

Ensina R.:

“Criminosos estão usando os sites de relacionamentos para propagar fotos com armas, vídeos enaltecendo o crime e incentivando o uso de drogas, fazendo clara apologia a diversos crimes e facções criminosas. Na maioria das vezes as imagens postadas servem como prova; e mesmo que as mensagens não sejam suficientes para constatar o delito, elas podem servir de pista para a polícia”²⁰.

No entender de P.²¹, os policiais do Rio de Janeiro prenderam na noite do dia 04 de outubro de 2012 um traficante que postou fotos em uma rede social portando armamento pesado. Em seu perfil, o jovem se vangloriava por estar sob efeito de drogas. Nas fotos o criminoso aparecia portando fuzis, granadas e pistolas no alto de um morro. Nas publicações ele se dizia integrante de uma facção e revelava a participação em confrontos contra criminosos de uma organização rival.

Ilustra M.²², que a mídia deu destaque a um caso de sequestro que aconteceu em 2010. Um estudante de 19 anos foi mantido refém em uma casa, a 150 quilômetros de Sorocaba, em Ilha Comprida, litoral sul paulista. Nove sequestradores foram presos. O que chamou a atenção da polícia nesse caso foi a forma como os sequestradores descobriram o perfil e a rotina das vítimas: a quadrilha escolhia as pessoas sem sair de casa. Tudo era feito pela internet.

²⁰ RODOTÀ, Stefano. **A vida na sociedade da vigilância. A privacidade hoje**. Rio de Janeiro: Renovar, 2008.

²¹ PAESANI, Líliliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 273.

²² MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.p. 290.

Segundo a polícia, os criminosos passavam horas e horas em sites de relacionamento, à procura de pessoas com sinais de riqueza. Os sequestradores olhavam principalmente as fotos, para saber, por exemplo, como era a casa da família e se a possível vítima fazia viagens para o exterior.

No entendimento de B.:

“O perigo de aceitar "amigos" estranhos on-line é justamente saber se este estranho é quem realmente se diz ser. Os usuários deixam à disposição seus perfis colocando em risco sua integridade física e de seus familiares. Sem muito esforço, os criminosos podem coletar interesses das pessoas, localização, movimentos e se estão fora de casa”²³.

Pondera M.²⁴, que: “na dúvida, é melhor reter a informação. Qualquer rede social, hoje, tem controles de privacidade. Você pode definir quem vai ver tal conteúdo, quem vai visualizar tais fotos. Desta forma, somente aquelas pessoas que você realmente conhece e que não vão comprometer você de nenhuma forma terão acesso”.

²³ BONAVIDES, Paulo. **Ciência política**. 12. ed. São Paulo: Malheiros, 2008.p. 265.

²⁴ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.p. 290.

CAPÍTULO II

2 - PRINCÍPIOS E GARANTIAS DO MARCO CIVIL

Ensina H.²⁵ que “o Marco Civil se inicia com o comando legal de que nele se estabelecem os princípios, garantias, direitos e deveres para o uso da internet no Brasil. Primeiramente, há que se ressaltar que tal comando pressupõe um equívoco do legislador e uma total dissonância do sistema jurídico em que se insere o Marco Civil. Quem estabelece princípios, garantias, direitos e deveres para quaisquer usos e tecnologias é a Constituição Federal do Brasil”.

Entende H.²⁶, que:

“O Marco Civil é uma legislação infraconstitucional que deveria implementar e regulamentar a Constituição. Contudo, não é isso que ocorre. Muitas linhas se seguirão abaixo para constatar que o Marco Civil repete descontextualizadamente princípios, garantias, direitos e deveres constitucionais sem aprofundá-los para as questões e problemas existentes de suas inserções nas tecnologias de informação e comunicação”.

No entender de P.:

“O Marco Civil gastou tintas e tintas para reeditar princípios e regulamentações já existentes no ordenamento jurídico e que, invariavelmente, já eram utilizadas para resolver questões e problemas de internet, como a vasta jurisprudência trazida neste trabalho”.¹⁷.

Ao constatar esse problema do Marco Civil, é necessário se indagar quais as perspectivas imaginadas pelo legislador ao se regular a internet.

Repisar modelos já prontos e desgastados não responde às problematizações surgidas pela exclusão digital, vigilantismo de governos e empresas, convergência da internet com as telecomunicações, crimes informáticos, manipulação de dados, uso indiscriminado de banco de dados, infrações de direitos autorais, produção de provas, devido processo legal, criptografia de dados etc.

Em sua doutrina P.²⁷, faz os seguintes questionamentos:

²⁵ HOBBSAWN, Eric. **A Era dos Extremos**. São Paulo: Saraiva, 2003, p. 123.

²⁶ HOBBSAWN, Eric. **A Era dos Extremos**. São Paulo: Saraiva, 2003, p. 124.

²⁷ PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 323.

Como o Marco Civil pretende enfrentar essas questões? Que sociedade virtual pensa o legislador? Quais questões surgidas com a tecnologia podem ser solucionadas com a normalização de regras? Como pensar o subsistema do Marco Civil dentro do sistema jurídico? Como foi pensado o diálogo entre as fontes? Como se pensar o governo e seus serviços como provedor de aplicações de internet?

Infelizmente, nenhuma dessas perguntas estruturais, que a legislação poderia construir, foi enfrentada. O Marco Civil quando fala em princípios, não conseguiu construir sentidos e valores em suas normas, pois desprovidas de perguntas necessárias a se pensar uma sociedade virtual mais justa e igualitária e que implemente novas cidadanias e negócios. Tudo isso foi esquecido.

Em sua definição de internet, C.²⁸ entende que:

Ao assumir somente uma definição técnica de internet, o Marco Civil fixou a legislação somente para regular o uso da ferramenta, ou seja, regula-se o meio e não os fins que são as pessoas e seus valores. A internet é símbolo de ser mais do que uma ferramenta, é um lugar de redes físicas para a comunhão de pessoas. Os protocolos lógicos somente identificam e viabilizam as conexões entre pessoas para se informarem, comunicarem e produzirem conhecimentos e ideias. A internet é o meio infinito de possibilidades e realizações humanas e não um fim em si mesmo.

Esse equívoco conceitual do Marco Civil da internet, que deveria ser das pessoas na internet, irradia-se sobre todas as suas normas e coloca quase sempre a perspectiva técnica em detrimento de valores a serem preservados, ressignificados e atualizados. Algumas normas do Marco Civil pecam excessivamente por argumentos técnicos, tal como o de neutralidade de rede (art. 9º),¹ e não dão respostas satisfatórias aos anseios da sociedade, por conta dos desvios argumentativos complexos e distantes do entendimento da maioria da população.

A utilização de conceituação técnica de internet serve para ampliar as exclusões sociais e digitais, pois se utilizam de discursos altamente especializados e restritivos, dominados por poucos e para poucos.

²⁸ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014, p. 269.

Dentro da coerência técnica desenvolvida pelo legislador do Marco Civil, as normas são diretrizes para os entes federativos. A perspectiva deveria ser outra, mais propositiva e menos programática. Porém, o Marco Civil não atualizou os princípios, garantias, direitos e deveres constitucionais, apenas os transcreveu sem enfrentamentos de suas contradições e perdas com relação às tecnologias de informação e comunicação.

Os entes federativos são parte importante do processo de aprofundamento das benesses da internet para todos os cidadãos. Através de suas participações, poderiam ser ampliados acessos e perspectivas de inclusões e conquistas sociais, entretanto, ao se reduzir a internet a normas programáticas, da forma como é pensada no Marco Civil, temos somente um aprofundamento das diferenças sociais na sua realidade virtual.

2.1 - Fundamentos Jurídicos do Marco Civil

A simples enumeração de princípios repetidos do que já foi instituído constitucionalmente é mera repetição sem contextualização com as práticas do que deveria a legislação pensar sobre qual internet ela quer para o país

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.

*Disciplina C.*²⁹, em sua doutrina, no dicionário *Houaiss*, tem várias

²⁹ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p.

acepções.¹ “O legislador escolheu esse termo no sentido de regulamento para o bem-estar social. Entretanto, tal acepção é falha e totalmente incoerente com a ideia de princípios a qual o artigo deveria fomentar. Regulamento de princípios sem construção e delineamento das práticas que os significam é meramente uma indicação de algo dissonante da realidade. Este *caput* já aponta os problemas axiológicos trazidos nos incisos abaixo e na conceituação equivocada de internet, tal como trazida anteriormente”.

No entender de C.³⁰: “disciplinar a internet não é somente dizer que se resguardará a proteção da privacidade. De qual privacidade estamos falando se não há uma lei de proteção de dados no país? A privacidade a ser garantida envolve questões de segurança de informação com a permissão de todos os usuários de internet terem acesso a criptografia de dados sem controle estatal? Quais são os limites para a formação de banco de dados dos entes federativos?”

No entendimento de B., liberdade de Manifestação do Pensamento e de Expressão:

“A disciplina do uso da internet no Brasil deve garantir a liberdade de expressão, comunicação e manifestação de pensamento, tal como determina a Constituição. Se já existe esta determinação na Constituição por quê repeti-la na lei infraconstitucional? Qual é o sentido? Devemos caminhar a interpretação em busca do que já foi construído ou estamos buscando algo novo? O objetivo desse trabalho é atualizar esses princípios a novas práticas de uma sociedade totalmente diversa daquela de 1988.”¹⁸

Assim, na exegese do que propõe o Marco Civil, deve-se analisar a liberdade de expressão, como “o direito de externar ideias, opiniões, juízos de valor, em suma, qualquer manifestação do pensamento humano”. P. B., aprofunda:

“O homem porém não vive concentrado só em seu espírito, não vive isolado, por isso mesmo que por sua natureza é um ente social. Ele tem a viva tendência e necessidade de expressar e trocar suas ideias

³⁰ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p.

¹⁸ BARRETO JUNIOR, Irineu Francisco. **A relevância do conceito sociedade da informação para a pesquisa jurídica**. In: PAESANI, Liliana Minardi. *Direito na sociedade da informação*. São Paulo: Atlas, 2007.p. 345.

¹⁹ BONAVIDES, Paulo. **Ciência política**. 12. ed. São Paulo: Malheiros, 2008.p. 303.

e opiniões com os outros homens, de cultivar mútuas relações, seria mesmo impossível vedar, porque fora para isso necessário dissolver e proibir a sociedade.”¹⁹

Para R.,³¹, “a Constituição, em posição contrária ao Marco Civil, adotou a liberdade de manifestação do pensamento em detrimento à liberdade de expressão. Nesse sentido, o art. 5o, inc. IV, da CF garante a liberdade de manifestação do pensamento, “sendo vedado o anonimato”. No art. 220, a Constituição determina que a “manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição”.

Não é somente a Constituição Federal que adotou esse conceito. A Convenção Americana de Direitos Humanos estipulou, em seu art. 13:

“Artigo 13 – Liberdade de pensamento e de expressão

1. Toda pessoa tem o direito à liberdade de pensamento e de expressão. Esse direito inclui a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, sem considerações de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha.”²⁰

Diante dessa consolidação constitucional do termo manifestação de pensamento, em que a liberdade de expressão é seu aspecto externo, nota-se que o legislador do Marco Civil, ao adotar os termos da Constituição, não a interpretou nas suas intenções e conteúdos dogmáticos, o que pode trazer confusões ao se interpretar o princípio da liberdade de manifestação do pensamento e de expressão na internet.

Assim, a liberdade de manifestação do pensamento tem como pressuposto o desenvolvimento dos direitos de personalidade, a fim de promover a livre circulação de ideias e o fortalecimento do Estado Democrático e Social de Direito. Somente com a liberdade de manifestação de pensamento assegurada é que se pode implementar outras garantias constitucionais e reafirmar a dignidade da pessoa humana. Contudo, a liberdade de manifestação de pensamento não é absoluta e tem os seus limites impostos por outras garantias.

Limites à Liberdade de Manifestação de Pensamento. A Convenção Americana de Direitos Humanos apresenta nos incisos do art. 13, inc. 2 a 5, as molduras dos limites da liberdade manifestação do pensamento em que

³¹ REALE, Miguel. Noções Preliminares de Direito. São Paulo: Saraiva, 2011, p. 210.

²⁰ Disponível em: <https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>

determina o seu sentido não absoluto.

A liberdade de manifestação de pensamento somente poderá ser exercida desde que respeite os direitos e reputação das demais pessoas, a segurança nacional, a ordem pública, ou da saúde ou da moral públicas, que não faça propaganda a favor da guerra, incite ao ódio nacional, racial ou religioso, discriminando e incitando ao crime e à violência.

Ensina H.³², “tal elenco de restrições impostas pela Convenção Americana de Direitos Humanos não podem ser assumidas também como absolutos. Conceitos como reputação, segurança nacional, ordem e moral pública são muito indeterminados e amplos para serem realmente critérios efetivos para a implementação das restrições ao direito de liberdade de manifestação de pensamento. Governos não democráticos e ditatoriais diuturnamente utilizam-se dos critérios de segurança nacional, ordem e moral pública para imporem censuras e cerceamento da liberdade de manifestação do pensamento de forma abusiva”.

A fim de diminuir a subjetividade de critérios tão amplos e incertos, P.³³, estipulou oito critérios de análise se há liberdade de manifestação de pensamento exercida nos limites constitucionais e da dignidade da pessoa humana. Toda a liberdade de manifestação de pensamento tem que adotar os seguintes parâmetros:

- a) fatos verdadeiros: a informação que goza de proteção constitucional é informação verdadeira;
- b) licitude do meio empregado na obtenção da informação: a Constituição veda obtenção de provas, conhecimentos ou informações que sejam obtidas por meios ilícitos. A liberdade de manifestação de pensamento não pode ser exercida por meio de um crime;
- c) personalidade pública ou estritamente privada da pessoa objeto da notícia: as pessoas que ocupam cargos públicos têm o seu direito de privacidade tutelado em intensidade mais branda, mas não quer dizer a sua supressão;
- d) local do fato: os fatos ocorridos em local reservado têm proteção mais ampla do que os acontecidos em locais públicos;
- e) natureza do fato: há fatos que são notícia (tremor de terra, terremoto, enchente), independentemente dos personagens envolvidos, mesmo quando exponham a intimidade, a honra ou a imagem de pessoas neles envolvidos;
- f) existência de interesse público na divulgação em tese: o interesse público na divulgação de qualquer fato verdadeiro se presume, desde que haja um interesse privado excepcional;
- g) preferência por sanções *a posteriori*, que não envolvam a proibição prévia da divulgação: que seja implementado o direito à liberdade de manifestação do pensamento e, se utilizado abusivamente, sanciona--se com

³² HOBBSAWN, Eric. A Era dos Extremos. São Paulo: Companhia das Letras, 2008, p. 149.

³³ PAESANI, Liliansa Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 345.

responsabilização civil ou penal de quem agiu ilicitamente. Sanções *a posteriori* somente serão aplicadas desde que da divulgação da liberdade de manifestação do pensamento acarrete um dano irreparável, tal como a divulgação de uma doença congênita muito pessoal”.³³

Com esses parâmetros é possível delinear caso a caso como explorar o direito à liberdade de manifestação de pensamento sem invadir direitos alheios, permeando possibilidades de aplicações práticas. E, quando houver dúvidas, preferir sempre a liberdade em detrimento da censura prévia.

Liberdade de Comunicação. Para A. S. F., a “liberdade de comunicação consiste num conjunto de direitos, formas, processos e veículos, que possibilitam a coordenação desembaraçada da criação, expressão e difusão do pensamento e da informação”.³⁴ A internet é um veículo de comunicação bidirecional em que se comunica e se informa automaticamente. Assim, o ato de se comunicar na internet, diferentemente das outras mídias, é também um direito de se manifestar o pensamento. Assim, trazer o direito de comunicação na disciplina na internet é uma tautologia morfológica com o direito à manifestação do pensamento.

Proibição de Censura Prévia. A liberdade de manifestação de pensamento é reforçada a todo tempo no Marco Civil numa luta diuturna contra a censura prévia de conteúdo na internet. Tanto isso é recorrente que o art. 19 do Marco Civil delinea essa opção de lutar contra a censura prévia (“com o intuito de assegurar a liberdade de expressão e impedir a censura”).

A censura prévia ocorre quando alguém, direta ou indiretamente, obsta, impede, exclui, opõe-se injustificadamente, fora das exceções constitucionais, à publicação de conteúdo, informação ou conhecimento, de áudio, vídeo ou texto, em determinada página de internet.

Para B.,³⁵ “A censura prévia em termos de internet não é somente uma questão de direitos e sim também de técnica, a qual o próprio Marco Civil reconhece nas questões de neutralidade de rede, em que a forma como a internet funciona e se desenvolve realiza por si só discriminações de conteúdos antes mesmo de serem publicados, independentemente da vontade de quem os publica. São inúmeros casos que os *sites* direcionam conteúdos para

³⁴ SIMÃO FILHO, Adalberto. **Sociedade da informação e seu lineamento jurídico**. In: PAESANI, Liliana Minardi (Coord.). *Direito na sociedade da informação*. São Paulo: Atlas, 2007.p. 256.

³⁵ BARRETO JUNIOR, Irineu Francisco. **A relevância do conceito sociedade da informação para a pesquisa**. In: PAESANI, Liliana Minardi. *Direito na sociedade da informação*. São Paulo: Atlas, 2007, p. 193.

determinados usuários geograficamente localizados, ou seja, uma pessoa de São Paulo pode ver o conteúdo e outra do Rio de Janeiro não.”

O *Google* tem diversas regras de relevância de conteúdo e que acabam por esconder outros, as quais os usuários nunca tenham acesso. Isso é uma forma de censura prévia indireta e que é coibida pelo art. 13.3 da Convenção Americana de Direitos Humanos:

“Não se pode restringir o direito de expressão por vias e meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões.”²³

No entendimento de C.³⁶, “a censura prévia tecnológica na internet, que foi ignorada pelo Marco Civil, ocorre em dois momentos: por meio de quem controla o código fonte dos *softwares*, no caso os provedores de aplicação de internet; e por quem controla a infraestrutura de telecomunicações”.

2.2 - Inclusão Social e Digital

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.*³⁷

Ensina C.³⁸, que promoção como objetivo do Marco Civil. “Promoção é o ato de promover que, no sentido do Marco Civil, significa dar execução aos princípios e direitos estabelecidos nos incisos inseridos no artigo. Os incisos do art. 4º não são *numerus clausus*, fechados. O Marco Civil, até mesmo por

³⁶ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 333.

³⁷ Disponível em:< https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm>

³⁸ CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 336.

conta de sua redação confusa e equívoca, deve permitir que novos objetivos, que não constaram da redação original, sejam construídos e apresentados nas decisões judiciais”.

No entendimento de P.³⁹, verifica-se que “a promoção será pautada pelos incisos e deverão orientar o legislador na formulação de políticas públicas e reinterpretação das leis vigentes. A partir do Marco Civil, algumas leis entrarão em contradição ou serão ampliadas no seu alcance. Por exemplo, o art. 154 da Lei Geral de Telecomunicações que versa sobre o compartilhamento de redes de telecomunicações poderá ser implementado para ampliar o acesso de todos à internet. Por outro lado, práticas e leis, que instituem obstáculos e empecilhos à implementação desses princípios deverão ser alteradas especificamente para questões de internet. Uma das leis que mais entram em conflito com o Marco Civil são relacionadas à propriedade intelectual”.

2.3 - Direitos dos Usuários de Internet

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

³⁹ PAESANI, Liliansa Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2013, p. 401.

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;⁴⁰

Para M.⁴¹ “o acesso à internet é essencial ao exercício da cidadania. O Marco Civil, no passo das legislações estrangeiras, incorporou a ideia de que o acesso à internet é direito do cidadão. Contudo, perdeu-se a oportunidade de se reafirmar valores e de ir além do reconhecimento do direito. O Marco Civil poderia ter caminhado, provocativamente, aos direitos fundamentais, já que discorre sobre vários deles. Mas não o fez. As legislações estrangeiras equiparam o acesso à internet como direito fundamental tão importante quanto a água, a eletricidade e ao direito de moradia”.

Entende C.,⁴² “errou-se no alvo também. Há um processo equívoco do legislador que estabelece direitos atrelados a tecnologias. Direitos são conquistas e necessidades históricas, construídas por processos e práticas sociais ao longo do tempo. Atribuir a uma tecnologia um direito seria o mesmo erro conceitual de se colocar o direito à informação ao jornal. Foi uma crítica reiterada que fiz na consulta pública que repetiu-se à

⁴⁰ Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>

⁴¹ MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre: Livraria do Advogado, 2012, p.314.

⁴² CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.p. 367.

exaustão por anos a fio. Infelizmente, essas críticas não foram ouvidas ou consideradas, já que o texto não atendeu aos objetivos da consulta pública de participação social na realização da lei”.

Contudo, ensina R., que:

“o acesso à internet se tornou essencial, mas não enfrentou as práticas de exclusão digital por falta de políticas públicas, questões econômicas, sociais, culturais e históricas, porque o problema não é a questão do acesso à internet”.⁴³

O alvo da luta pelos direitos é outro bem longe da simples questão do acesso à internet. Ter acesso à internet não significa o exercício da cidadania, pois existem cidadãos que têm o acesso à internet, mas não conseguem exercer a cidadania, pois, por exemplo, o provedor de aplicações de internet não tem um *site* adaptado a pessoas com deficiência visual.

Complementa R.⁴⁴, que “o acesso à internet não é essencial ao exercício da cidadania, somente sendo mais um caminho dela, que, se não implementada, duplica a distância dos que têm para os que não têm. Direitos dos usuários de internet. Apesar da falta de diálogo do Marco Civil com o Código de Defesa do Consumidor, os direitos estipulados nos incisos não são exaustivos e sim ampliativos dos que são assegurados na legislação consumerista, que serviu de base para muito do que a jurisprudência já decidiu sobre a internet no Brasil”.

Sobre os direitos ampliados com o Marco Civil P.:

“Assim, o que se estipula nesse *caput* é uma ampliação dos direitos que já existem no ordenamento jurídico. A defesa dos usuários e/ou consumidores de internet deve ter como foco uma análise sistêmica em que devem se incluir as leis que possam ampliar a proteção deles. Conforme se apura da interpretação do Marco Civil, há nítida preferência do legislador pela defesa do usuário, hipossuficiente nas relações tecnológicas, nos usos de seus dados pessoais e profissionais”⁴⁵.

Contudo, ensina R.⁴⁶ “nessa questão de dados pessoais, o usuário não

⁴³ REALE, Miguel. **Noções Preliminares de Direito**. São Paulo: Saraiva, 2011.p. 199.

⁴⁴ REALE, Miguel. **Noções Preliminares de Direito**. São Paulo: Saraiva, 2011.p. 199.

⁴⁵ PAESANI, Líliliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.p. 400.

⁴⁶ REALE, Miguel. **Noções Preliminares de Direito**. São Paulo: Saraiva, 2011.p. 354.

possui um requisito importante: não há transparência no uso dos dados pessoais fornecidos pelos usuários, mesmo que juridicamente exista uma garantia de que eles não serão usados comercialmente. Na prática, o funcionamento das empresas de telecomunicações e dos provedores de acesso e de aplicações à internet não possuem procedimentos claros sobre a guarda e conservação das informações fornecidas pelos usuários. Nem o Marco Civil determina como serão esses procedimentos. E não dá para se garantir direitos sem existirem regras claras e definidas sobre como funcionam os sistemas e tecnologias de informação e comunicação”.

CAPÍTULO III

3 – CRIMES CIBERNÉTICOS E A FRAGILIDADE DA LEI 12.737/12

Este capítulo irá tratar sobre a definição de crimes virtuais, demonstrando sua incidência no cenário nacional e internacional, sendo demonstrado ainda, os riscos decorrentes destas práticas da era moderna digital.

A. B., descreve em seu livro *Direito Penal Informático*, sobre a deficiência que se tem quanto aos crimes praticados no ambiente virtual, fazendo ainda uma referência a sociedade de informação:

É comum ouvir-se que o “Direito é o reflexo da sociedade”, porém, muito pouco de se tem observado de efetivas mudanças para que essa afirmação deixe de ser um mero argumento e retórica. Se a sociedade vive na era da informação ou era digital deve, efetivamente, contemporizar com essa situação.⁴⁷

Ademais, será evidenciada a fragilidade da Lei 12.737/12, popularmente conhecida como “Lei Carolina Dieckemann”, norma esta que fora inserida em nosso ordenamento jurídico, para sanar uma lacuna existente neste último, no que diz respeito aos crimes praticados através da internet.

3.1- DOS CRIMES CIBERNÉTICOS

Definem-se crimes cibernéticos, as condutas delituosas praticadas através do uso de computadores ou outro dispositivo informático similar provocando danos na esfera social.⁴⁸ Pode-se dizer que é a ação praticada

⁴⁷ BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013. p. 169

⁴⁸ WENDT, Emerson; JORGE; Higor Vinicius Nogueira. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. 2. Ed. Rio de Janeiro: Brasport, 2013.p. 18.

através do mundo abstrato ou virtual com consequências no mundo real. Ainda como complemento, deve-se definir que o crime poderá utilizar dispositivo informático, tanto como instrumento para concretizar o delito, ou ser ele, objeto da ação.⁴⁹

F. define ainda, crime informático como “toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão”.⁵⁰

3.2- CONSIDERAÇÕES SOBRE CRIME

A definição de crime pode ser dividida em diversos aspectos, a saber: dentro do aspecto material quando determinada conduta deve ser considerada como crime ou não, ou seja, é a essência do conceito de crime, sendo crime, no entanto, toda atitude humana, sendo ela omissiva ou comissiva que cause lesão ao patrimônio jurídico da sociedade. Será formal todo ato que o legislador assim o dispuser; estando a prática tipificada como crime, assim será o mesmo considerado. E por fim, analítico, quando se aplica uma análise maior do caso, observando se tal ato é considerado típico ou ilícito, observando ainda, a tipicidade da conduta e só então decidindo se a mesma é lícita ou não.⁵¹

Ao legislar sobre este assunto, qual seja, a definição do que vem a ser crime, cabe ao Poder Legislativo um cuidado maior, pois a Constituição Federal, em seu artigo quinto, dispõe da seguinte maneira: “não há crime sem Lei anterior que o defina, nem pena sem prévia cominação legal”⁵², bem como tal disposição se encontra no artigo primeiro do Código Penal Brasileiro. Portanto, sendo assim, a pessoa que praticar algum ato que cause uma lesão à sociedade, tal ato só será punido caso esteja previamente configurado como crime na legislação.

Sobre este aspecto, tem-se o entendimento de P. M.:

Há em nossos dias perigosa adaptação dos princípios constitucionais, não podendo a garantia enunciada ser meramente formal. A descrição há de ser específica e individualizada do comportamento

⁴⁹ VELLOZO, Jean Pablo Barbosa. **Crimes Informáticos e criminalidade contemporânea**. Disponível em: <<http://jus.com.br/artigos/44400/crimes-informaticos-criminalidade-contemporanea/1>>. Acesso em 29 de outubro de 2019.

⁵⁰ FERREIRA, Ivete Sensive. **A criminalidade Informática**. Bauru: Edipro, 2000. P. 210.

⁵¹ CAPEZ, Fernando. **Curso de Direito Penal: Parte Geral**. V.1.16 ed. São Paulo: Saraiva, 2012. 125

⁵² BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituição/Constituição.htm>. Acesso em 01 de novembro de 2019.

criminoso, sob pena de não trazer uma garantia real e efetiva. Não há como se conceber uma lei excessivamente genérica em matéria penal. Deve ser perseguida de perto a identificação de cada comportamento que se tenha como delituoso, evitando-se assim, a arbitrariedade nociva, ameaça grave às liberdades individuais.⁵³

Tendo em vista essa consideração, fica, no entanto o legislador incumbido de ser ágil e coerente na formulação de dispositivos que atuem dando a devida proteção ao cidadão que age de forma correta no meio social.

3.2.1- DO USO DA ANALOGIA

A analogia (aplicabilidade a uma hipótese não regulada por lei disposição relativa a um caso semelhante)⁵⁴ esta será utilizada em situações onde o caso concreto não dispuser de uma lei específica que dê amparo ao anseio social, cabendo assim, o operador do direito é um caso semelhante sanar este lapso existente se utilizando da analogia para tanto.

Além do mais, B., citado por D. J., dispõe que a respeito desse fator, o que acontece de fato é: “a aplicação ao caso a ser decidido de norma ou regra que regula hipótese semelhante em matéria análoga; pela regulamentação de caso análogo, infere-se que o legislador comportar-se-ia da mesma maneira se tivesse previsto o caso que na norma não se enquadra”.⁵⁵

No que diz respeito à aplicabilidade na analogia no direito penal, cabe ressaltar que na espécie “*in bonam partem*” é aceita e aplicável a analogia, pois a mesma será usada para beneficiar o agente. Porém, no que se refere a espécie “*in malam partem*”, Damásio de Jesus considera inadmissível a aplicabilidade da analogia a ser usada em norma penal incriminadora³⁶, uma vez que, não se pode violar o princípio da reserva legal em prejuízo do agente, portanto nessa modalidade não se deve ser utilizada a analogia, assim se posiciona Fernando Capez sobre o assunto em comentário:

Imagine considerar típico o furto de uso (subtração de coisa alheia móvel para uso), por força da aplicação da analógica do art. 155 do Código Penal (subtrair coisa alheia móvel com ânimo de assenhoramento definitivo). Neste caso, um fato não considerado criminoso pela lei passaria a sê-lo, em vidente afronta ao princípio constitucional do art. 5º, XXXIX (reserva legal). A analogia *in bonam*

⁵³ LIMA, Paulo Marco Ferreira. **Crime de Computador e Segurança Computacional**. 2. Ed. São Paulo: Atlas, 2013. P. 14.

⁵⁴ CAPEZ, Fernando. **Curso de Direito Penal: Parte Geral**. V. 1. 16 ed. São Paulo: Saraiva, 2012. P. 49

⁵⁵ BATTAGLINI, apud, JESUS, Damásio E. de. **Direito Penal**. São Paulo: Saraiva, 2003. P. 50

partem, em princípio seria impossível, pois jamais será benéfica ao acusado a incriminação de um fato atípico.³⁷

Ainda em relação a esta questão, Mirabete ainda complementa dizendo que é reprovável a utilização da analogia com a finalidade da criação de ilícitos penais ou para estabelecer sanções criminais.³⁸

Por fim, feitas estas considerações, cabe ressaltar agora o importante cuidado que cabe aos legisladores, pois, nas palavras de Paulo Lima, “a internet não pode ser entendida como uma terra “sem lei”, devido às ligações que decorrem dela sempre serem respaldadas em relações entre seres humanos devendo assim existir um suporte eficaz por parte do Estado evitando que ações nefastas sejam praticadas³⁹, ou quando tal ação vier a acontecer, aqueles que sofrerem com o delito não venha a ficar desamparado e sem uma resposta efetiva or parte do Estado.

3.3- ALGUMAS CONSIDERAÇÕES SOBRE A LEI 12.737/12 E EXPOSIÇÃO DE SEUS MOTIVOS

A Lei 12.737/12, anterior Projeto de Lei nº 2793/2011, fora criada para tipificar condutas criminosas praticadas através da rede de computadores, dando assim, um amparo a aquelas pessoas que sofressem com tal invasão e também coibindo assim a tentativa de novos atos como estes.

Antes de adentrarmos a mais neste contexto da Lei 12.737/12, cabe ressaltar, brevemente, a respeito do “Caso Carolina Dieckemann”, caso este que, deu ensejo à criação da referida Lei. No ano de 2012 a atriz Carolina Dieckemann teve sua intimidade violada e exposta na internet. A princípio a atriz suspeitava ter sido funcionários de uma loja de infomática que praticaram tal delito, pois a atriz havia levado seu computador portátil para que fizessem um reparo no mesmo. Dois meses após este evento, a atriz foi contatada por pessoas que diziam estar em posse de suas fotos íntimas e que iria expô-la, caso a mesma não pagasse a quantia de dez mil reais. De início a atriz tentou resolver esta situação de forma sigilosa para exposições.⁵⁶

No dia sete de maio do ano de 2012, Carolina Dieckemann foi até a delegacia expor o caso para que fosse, então, iniciada a investigação do caso, pois três dias antes de divulgarem suas fotos íntimas, haviam sido divulgadas também, fotos de seu filho menor em alguns sites.

⁵⁶ G1. **Carolina Dieckemann fala pela 1ª vez sobre fotos e diz que espera Justiça.** Disponível em: <<http://g1.com/pop-arte/notícia/2012/05/carolina-dieckemann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html>>. Acesso em 30 de outubro de 2019.

Ao final da investigação, conclui-se que não haviam sido os funcionários da loja de informática que haviam copiado as fotos da atriz, mas sim um grupo de *Crackers* (diferente de *hackers*, uma vez que, estes são pessoas que buscam aperfeiçoar e proteger dispositivos informáticos e aqueles, usam seus conhecimentos apenas para o mal, ou seja, para práticas ilícitas⁵⁷) que conseguiram acessar o email da atriz e subtraíram suas fotos e posteriormente as divulgaram.

Tais fatos causaram uma comoção e alerta nacional devido à intensa pressão da mídia que não apenas evidenciou a fragilidade que o Brasil tinha quanto à proteção do indivíduo em sua esfera privada, mas também aos danos que tal exposição podem causar.

A exposição de motivos da Lei 12.737/12 a respeito da Lei Azeredo:

Ao nosso ver, o PL 84/1999, em sua redação atual, traz propostas de criminalização demasiadamente abertas e desproporcionais, capazes de ensejar a tipificação criminal de condutas corriqueiras praticadas por grande parte da população na Internet. Tal estratégia redacional, típica de uma sociedade de risco de uma lógica de direito penal do inimigo, busca uma antecipação da tutela penal a esferas anteriores ao dano, envolvendo a flexibilização das regras de causalidade, a tipificação de condutas tidas como irrelevantes, a ampliação e a desproporcionalidade das penas e a criação de delitos de perigo abstrato, dentre outras características.⁵⁸

A mencionada Lei, que posteriormente se tornaria o Projeto Lei nº 89/2003, ao ir para o Senado, iria punir desta forma, atitudes que não carecem de repressão penal, como por exemplo, testes de segurança, não autorizados, de sistemas informáticos, mas que houve prévio anúncio, ou seja, ações que não possuem a intenção ou a finalidade de praticar um crime, mas pelo contrário, intensões benéficas, seriam punidas.

Paralelo a Lei 12.737/12 ou como era popularmente chamada, Carolina Dieckemann. Devido a inúmeras transformações sofridas pela Lei 84/99 não havia mais como ser alterada, desta forma alguns temas que não foram tratados neste projeto, como pontua o texto da exposição de motivos da referida lei:

Ocorre que, em seu atual estágio de tramitação, por conta de questões regimentais, o Projeto e Lei referido não pode mais ser emendado ou alterado. Apresentamos, portanto, nossa proposta alternativa de criação de tipos penais específicos para o ambiente da

⁵⁷ Redação Olhar Digital. **Qual a diferença entre hacker e cracker?**. Disponível em: <http://olhardigital.uou.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024>. Acesso em 28 de outubro de 2019

⁵⁸ BRASIL. **PROJETO DE LEI 2793 DE 2011**. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostraintegra?codteor=944218&filename=P L+2793/2011>. Acesso em 30 de outubro de 2019.

Internet. Esta redação que apresentamos, e que ainda é passível de aperfeiçoamento e contribuições- sempre de forma a garantir os direitos do cidadão na Internet e evitar a criminalização de condutas legítimas e corriqueiras na Internet.⁵⁹

A referida Lei propôs um equilíbrio das penas em consonância com a prática ilícita efetuada pelo agente delituoso. Cabendo ressaltar ainda que, um dos objetivos, segundo a justificativa da mesma, é estabelecer uma harmonia entre ela com as já existentes no ordenamento jurídico.

A referida Lei foi sancionada em 02 de dezembro de 2012 pela ex Presidenta Dilma Rousseff. Proveniente do Projeto de Lei 2.793 do ano de 2011 apresentado em 29 de novembro de 2011, pelo Deputado Paulo Teixeira, que tramitou em regime de urgência e em tempo célere no Congresso Nacional, em comparação com outros projetos sobre delitos informáticos que as casas de leis apreciavam, como por exemplo, o Projeto Lei 84/1999, a “Lei Azeredo”, também transformado em lei ordinária 12.735/2012 em 3 de dezembro de 2012.

Talvez, a tramitação acelerada da mencionada lei, com o intuito de dar uma resposta à sociedade com maior permanência, dadas as circunstâncias daquele momento vivido no País, é que não se teve um tempo de manutenção necessária para a lei incorporar e tornar uma ferramenta com maior poder para coibir os crimes nela previstos também aprofundar mais nesta matéria.

3.4- ANÁLISE DA MATÉRIA TRATADA NA LEI 12.737/12

Conforme, o até aqui exposto, resta-se claro que, muitas são as tentativas do Estado, mediante as normatizações já existentes, para tratar as mais variadas ações nos ambientes virtuais. Entretanto, apesar de ser algo evidente em nosso dia a dia, o legislador pátrio não consegue evoluir e criar dispositivos com a mesma celeridade da empregada pela sociedade em suas transformações, logo, o legislador acaba pecando em relação à celeridade em que oferece um amparo legislativo.

Cabendo, apontar ainda o reconhecimento que a sociedade está sempre a evoluir, se modificar, em diversas épocas, ela tende a se comportar de

⁵⁹ BRASIL. PROJETO DE LEI 2793 DE 2011. Disponível em: <http://www.camara.gov.br/proposicoes/Web/prop_mostraintegra?codteor=944218&filename=PL+2793/2011>. Acesso em 30 de outubro de 2019.

alguma determinada forma.

Neste sentido, cabe ressaltar L. M. P. que:

Vivemos em uma época em que a produção normativa é insuficiente tanto para fazer frente às mudanças sociais, causadas pelo rápido avanço tecnológico, como para obter sua legitimação diante de grupos sociais cada vez mais fracionadas, que não compartilham seus valores com os demais e encontram um dos poucos pontos de contato justamente no próprio avanço tecnológico, notadamente na internet.⁶⁰

Contudo, apesar de o propósito aqui seja fazer uma breve crítica ao Estado, e apontar uma possível omissão, ainda que esta seja parcial, no que se refere aos crimes virtuais, há que se mencionar que o mínimo apresentado por parte do Estado, é a própria Lei 12.737/12, que já é um grande avanço para a sociedade.

A mencionada lei foi alvo de muitas críticas entre juristas e especialistas pois seus dispositivos são amplos, confusos e podem gerar dupla interpretação, o que pode ser utilizado para enquadramento criminal de condutas triviais ou mesmo para a defesa e respaldo dos infratores cibernéticos, que tornaria a lei injusta e ineficaz. Sob outro prisma, ainda, as penas são pouco inibidoras.

Com o advento dessa nova lei, o Código Penal Brasileiro foi modificado em quatro artigos, sendo eles: o artigo 154, violação do segredo profissional, que agora possui o artigo 154- A, que dispõe sobre a invasão de dispositivo informático alheio. E artigo 154- B que serve como um complemento do artigo anterior, neste ficou definido que a ação penal será pública mediante representação, salvo se o delito tenha sido contra a administração pública direta ou indireta.

Pois bem, o artigo 154- A, versa sobre a invasão de dispositivos informáticos versando:

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 de titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
Pena- detenção, de 3 (três) meses a 1 (um) ano, e multa.⁶¹

Neste artigo, está tutelado a intimidade, a vida privada e o direito ao sigilo de dados constantes em dispositivos informáticos. Há também, ao final

⁶⁰ PAESANI, Liliansa Minardi (Coord). **O direito na sociedade de informação**. São Paulo: Atlas, 2007.

⁶¹ Disponível em: <http://www.planalto.gov.br/ccvil_03/decreto-lei/Del2848compilado.htm>. Acesso em 02 de novembro de 2019.

do caput, do patrimônio do titular do dispositivo violado, punindo a intencionalidade de obtenção de vantagem ilícita, ao agir, instalando vulnerabilidade no dispositivo da vítima.

O núcleo central da conduta típica, se consubstância no verbo “invadir”⁶²⁴⁶ e “ingressa virtualmente, sem autorização expressa ou tácita do titular do dispositivo”. Portanto, o crime consiste em invadir computadores, *tablets, smartphone, HD's*, instalando programas ou conectando a outros dispositivos e não necessariamente precisa estar conectado à internet.

Preconiza C., ainda que:

A invasão deve se dar por meio de violação indevida de mecanismo de segurança estabelecido pelo usuário do dispositivo. Como exemplo de segurança, podemos citar; firewall, antivírus, antimalware, antispyware, senha restrita para acesso pessoal de usuário e etc.^{63 47}

A finalidade no presente caso seria de buscar a obtenção, a adulteração ou a destruição de dados ou informações, sem este elemento o crime não se aperfeiçoa. No tocante a este caput, C. aponta uma polêmica, e ainda alega que existe ali uma redação com diferentes interpretações, uma vez que, ao final do caput é descrita a conduta de instalar vulnerabilidades para obter vantagem ilícita, passando assim, a existir duas descrições típicas distintas, quais sejam, a já mencionada de invasão de dispositivo, com o fim de obter, adulterar ou destruir dados ou informações, como também, o de instalar vulnerabilidades para os fins de obtenção de vantagem ilícita. Neste último, o crime se aperfeiçoa somente com a instalação de vulnerabilidades, não sendo, portanto, a ocorrência da obtenção de vantagem ilícita; já no primeiro caso, a consumação se dá no simples fato de invadir, mesmo que não haja a obtenção, adulteração e destruição de dados, ambas as condutas são crimes formais.

Ante todo o exposto acima, C., alega que:

Pode surgir também a interpretação de que só há um verbo no tipo penal, consistente na ação de invadir. Nesta hipótese, a invasão se daria com o fim especial de: (a) obter, adulterar, ou destruir dados; (b) instalar vulnerabilidade apenas um crime, portanto. É crime formal. A parte final, nessa hipótese, seria apenas mais sobre as finalidades exigidas pelo tipo penal (invadir dispositivo informático com o fim de instalar vulnerabilidades).⁶⁴

⁶² CAPEZ, Fernando. **Código Penal Comentado**. Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 347.

⁶³ CAPEZ, Fernando. **Código Penal Comentado**. Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 347.

⁶⁴ CAPEZ, Fernando. **Código Penal Comentado**. Fernando Capez, Stela Prado. - 6. Ed.- São Paulo: Saraiva, 2015. P. 348

Portanto, dá-se no entendimento de haver dois crimes distintos, primeiro o agente invade dispositivo alheio com o fim de obter, adulterar ou destruir dados e posteriormente instala vulnerabilidades com o fim especial de obter vantagem ilícita.

3.5 – DA FRAGILIDADE DA LEI 12.737/12

Ao analisarmos a matéria tratada no dispositivo legal acima mencionado, encontramos uma série de falhas em sua redação, falhas estas que trazem como atípicas algumas condutas que pode ser praticadas por cibercriminosos.

O tema em foco do presente trabalho se encontra no artigo 154-A da referida lei, que discorre da seguinte maneira em seu caput:

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.⁶⁵⁴⁹

O que define sujeito ativo e passivo está bem no início do artigo, no trecho em que diz “Invadir dispositivo informático alheio”, invadir aqui, de acordo com os ensinamentos de R. G. se traduz em, violar, penetrar ou acessar.⁶⁶ Com isso, sujeito ativo, neste caso, é aquele que invade um dispositivo informático alheio, e o sujeito passivo, é quem sofreu a lesão.

No que diz respeito a isso, T. V. e F. M. ensinam que o legislador ao optar pela expressão “invadir dispositivo informático alheio”, acaba tornando atípica as condutas daquele que invadir dispositivo próprio para obter, indevidamente, dados alheios que lá estejam armazenados.⁶⁷

Sendo assim, aqueles que acessam uma “*lan house*”, um computador de uma empresa, ou qualquer outro dispositivo de terceiros, está com sua privacidade em risco, pois o proprietário do dispositivo informático poderá ter acesso a informações que ali possam estar contidas. Como por exemplo, um empregador que pode acessar o dispositivo informático que seu empregado

⁶⁵ BRASIL. **Código Penal.** Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 12 de novembro de 2019.

⁶⁶ GRECO, Rogério. **Código Penal Comentado.** 7. Ed. Niterói: Impetrus, 2013. P. 443.

⁶⁷ VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos.** Belo Horizonte: Fórum, 2013. P. 94.

usou e, senso assim, usar as informações que ali existam.

T. V., ensina a esse respeito:

Trata-se obviamente de uma situação absurda, pois o que se deve tutelar é a inviolabilidade dos dados, independentemente de quem seja o proprietário da máquina. Não há, porém, como o intérprete sanar o problema, pois a analogia in marlam partem é vedada no Direito Penal pelo princípio constitucional da legalidade. Espera-se, pois, que o legislador corrija esta lacuna por meio de uma nova lei.⁶⁸

52

A lacuna do artigo mencionado, não se limita no que fora dito acima, mas torna-se cada vez mais incongruente ao exigir a presença de um mecanismo de segurança e bem como, sua indevida violação para que, assim, seja tipificado o crime.

R. G. discorre que “essa exigência, isto é, a violação indevida de mecanismo de segurança, impede que alguém seja punido pelo tipo penal previsto pelo art. 154-A”.⁶⁸

Tal condição para que o delito possa ser caracterizado, embora ao ser criado tivesse uma blindagem de boas intenções, de acordo com a exposição de circunstâncias já apresentado, deixou muito frágil o objeto repressivo da lei, criando mais condutas atípicas.

T. V., assim discorre:

O elemento normativo “mediante violação indevida de mecanismo de segurança” faz com que seja atípica a conduta quando o dispositivo informático não possuir qualquer mecanismo de segurança, tais como senhas de acesso, antivírus, firewalls ou similares. É imprescindível que o agente supere este obstáculo tecnológico para que a conduta seja tipificada.⁶⁹

O absurdo dessa exigência, qual seja “violação indevida de mecanismo de segurança” mostra claramente a ausência de conhecimento do legislador. Essa lei não considerou que uma grande parcela da população ainda não tem conhecimento do grande avanço que ocorreu nos últimos tempos, e relação a rede mundial de computadores trouxe, assim, não os protegendo quando faz estas exigências supracitadas para configurar o crime.

Assim, resta-se claro então, o risco eminente que corre as pessoas que ainda não acompanharam esse avanço tecnológico, no que diz respeito a sua intimidade e vida privada. Vivemos, hoje, em um cenário onde o avanço

⁶⁸ VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos**. Belo Horizonte: Fórum, 2013. P. 95.

⁶⁹ GRECO, Rogério. **Código Penal Comentado**. 7. Ed. Niterói: Impetrus, 2013. P. 444.

datecnologia se torna real e necessário para nosso meio, e paralelo a isso espera-se que o Estado dê a preservação dos direitos conquistados há bastante tempo, podendo assim atuar de forma eficiente em sua manutenção.

A pena para aqueles que praticam os atos descritos no caput do artigo 154-A do Código Penal, assim como, aquele que oferece, distribui, vende ou difunde programa que facilite ou faça a prática descrita no caput, se realizada será pena de detenção de três meses a um ano, ou multa.

O Centro de Apoio Operacional Criminal do Ministério Público de São Paulo, afirma ainda que a mencionada lei possui deficiências que deixam frágeis a obtenção de uma resposta por parte do Estado, tendo em vista os ataques cibernéticos, deficiências estas que vão muito além de uma má redação, mas também se estende a má elaboração da pena a ser aplicada:

Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexibilidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo).⁷⁰

Conforme todo o demonstrado até o presente momento, os crimes virtuais estão se tornando, cada vez mais, uma realidade devido ao acesso e o combate contra os agentes criminosos, não é feito de forma simples e de fácil solução para tal problema, demanda uma investigação bem apurada e muito eficiente.

Encerra o Ministério Público de São Paulo, afirmando que a Lei 12.737/12 não consegue, por si só, desestimular aqueles que abusam das facilidades tecnológicas, bem como não é capaz de investigar e chegar até aqueles que praticam tais atos ilícitos usando da internet e dispositivos informáticos.

O parágrafo primeiro do artigo 154-A, “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”, também possui uma lacuna em sua disposição legal, tendo em vista que, a ação penal do crime, seja aquele definido no caput, ou no parágrafo primeiro,

⁷⁰ Ministério Público de São Paulo. **Novas Leis de crimes cibernéticos entra em vigor.**

Centro de Apoio Operacional Criminal. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_crimina/ notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR>. pdf. Acesso em: 05 de novembro de 2019.

estabelecido pelo artigo 154-B, define que tais crimes somente se procederão mediante representação da vítima, exceto em algumas hipóteses relacionadas a Administração Pública direta ou indireta.

De acordo com R. S., a vítima definida no parágrafo primeiro é indeterminada, tendo em vista que, diferente do caput, onde neste último a vítima é facilmente identificada, no presente caso, não tem como se definir quem foi a vítima, pois a punição cairá sobre aquele que vende programa que facilita o crime descrito no caput. Sendo assim, não conseguindo existir tal definição, como se procederá a punição penal, já que a vítima deverá fazer a representação?⁷¹

R. S., ensina ainda que existem duas correntes para este caso, a primeira diz que tal parágrafo é letra morta, pois houve desatenção do legislador por não ter previsto a possibilidade da ação penal pública incondicionada; a segunda corrente afirma que no silêncio do legislador deverá se proceder com a ação penal pública incondicionada.⁷²

Sendo assim, restou claro o quão complexo é o artigo da referida lei, e na mesma medida, o quão falha é sua redação, deixando uma lacuna em questões que deveriam ser tratadas de forma diferente, e não conseguindo agir de forma efetiva na proteção da dignidade da pessoa humana, bem como, em sua privacidade.

⁷¹ CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2019.

⁷² CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2019.

CONSIDERAÇÕES FINAIS

Graças à era da Internet móvel e dos *smarphones*, o futuro sem computador está em andamento e se projetam aparelhos em que nem as mãos serão utilizadas para interagir com os novos sistemas. Esses aparelhos podem ser o início da era em que o homem e a máquina podem se fundir de fato.

Sem a presença de uma tutela significativa em relação ao conjunto de informações recolhidas a nosso respeito pelas inovações tecnológicas dos sistemas inteligentes, toma-se difícil preservar a privacidade e a dignidade sem reduzi-las a "mercadorias". Como consequência, sente-se a necessidade de eliminar a ingerência de elementos externos na esfera privada das pessoas.

E reconduzindo o pensamento de R. quando afirma: "nós somos os nossos *gens*, nós somos os nossos dados". Essas afirmações representam, sem dúvida, a realidade e ao mesmo tempo conduzem a um reducionismo cultural inaceitável, pois somos também a nossa cultura, as nossas relações com os outros, o nosso viver num espaço histórico e ambiental. Nesse contexto, como preservar a integridade da esfera privada do indivíduo? Hoje, esse direito é reconhecido como fundamental de uma identidade humana em confronto constante com uma tecnologia sempre mais invasiva.

Como consequência da atual realidade, sem uma tutela do "corpo eletrônico", o conjunto das nossas informações pessoais, a própria liberdade pessoal está em perigo e se abre espaço para a construção de uma sociedade da vigilância, da classificação e da seleção social. Como consequência, se torna evidente que a tutela da privacidade se revela como sendo o instrumento necessário para a defesa da sociedade da liberdade.

As opiniões sobre o projeto da Lei de Crimes de Informática estão divididas, tanto no que concerne à utilidade de se editar nova lei para tratar de situações já previstas na legislação brasileira, como no que tange ao cadastramento e ao ônus imposto aos provedores de serviços na internet. Parece certo que, com o referido cadastramento, não se pretende autorizar o provedor ou o Estado a interferir na liberdade dos usuários, seja monitorando o teor das mensagens eletrônicas, bloqueando o acesso à rede ou censurando o conteúdo disponível na internet.

A questão da liberdade de expressão merece atenção especial. Não nos parece que o cadastramento dos usuários venha a cercear a livre

manifestação do pensamento, que é garantia fundamental do cidadão, conforme previsto no artigo 5º, inciso IV, da Constituição da República Federativa do Brasil, até mesmo porque ela só pode ser exercida mediante identificação.

REFERÊNCIAS

ASCENÇÃO, José de Oliveira. **Direito da Internet e da sociedade da informação**. Rio de Janeiro: Forense, 2002.

BARRETO JUNIOR, Irineu Francisco. **A relevância do conceito sociedade da informação para a pesquisa jurídica**. In: PAESANI, Liliana Minardi. *Direito na sociedade da informação*. São Paulo: Atlas, 2007.

BATTAGLINI, apud, JESUS, Damásio E. de. **Direito Penal**. São Paulo: Saraiva, 2003.

BONAVIDES, Paulo. **Ciência política**. 12. ed. São Paulo: Malheiros, 2008

BRASIL. **Constituição da República Federativa do Brasil de 1988**.

Disponível em:

<http://www.planalto.gov.br/ccivil_03/Constituição/Constituição.htm>. Acesso em 01 de novembro de 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado, 1988.

BRASIL. **PROJETO DE LEI 2793 DE 2011**. Disponível em:

<http://www.camara.gov.br/proposiçõesWeb/prop_mostraintegra?codteor=944218&filename=PL+2793/2011>. Acesso em 30 de outubro de 2019.

BRASIL. **Código Penal**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em 12 de novembro de 2019.

BRITO, Auriney. **Direito Penal Informático**. São Paulo: Saraiva, 2013.

CAPEZ, Fernando. **Código Penal Comentado**. Fernando Capez, Stela Prado.- 6. Ed.- São Paulo: Saraiva, 2015.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. Rio de Janeiro: Brasport, 2014.

CUNHA, Rogério Sanches. **Art. 154- A CP: Violação de segredo profissional**. Disponível em: <http://www.youtube.com/watch?v=YcOv-yv_H2c>. Acesso em: 08 de novembro de 2019.

DINIZ, Mareio Augusto de Vasconcelos. **Controle de constitucionalidade e teoria da recepção**. São Paulo: Malheiros, 2003.

FERREIRA, Ivete Sensive. **A criminalidade Informática**. Bauru: Edipro, 2000.

G1. **Carolina Dieckemann fala pela 1ª vez sobre fotos e diz que espera Justiça.** Disponível em: <[HTTP://g1.com/pop-arte/noticia/2012/05/carolina-dieckemann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html](http://g1.com/pop-arte/noticia/2012/05/carolina-dieckemann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html)>. Acesso em 30 de outubro de 2019.

GRECO, Rogério. **Código Penal Comentado**. 7. ed. Niterói: Impetus, 2013.

HOBBSAWM, Eric. **A Era dos Extremos**. São Paulo: Companhia das Letras, 2008

JESUS, Damásio E. de. **Direito Penal**. São Paulo: Saraiva, 2003.

LIMA. Paulo Marco Ferreira. **Crime de Computador e Segurança Computacional**. 2. Ed. São Paulo: Atlas, 2013.

MARQUES, Jader. **O Direito na Era Digital**. Porto Alegre; Livraria do Advogado, 2012.

Ministério Público de São Paulo. **Novas Leis de crimes cibernéticos entra em vigor**. Centro de Apoio Operacional Criminal. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR>. pdf. Acesso em: 05 de novembro de 2019.

MIRABETE, Julio Fabbrini. **Manual de Direito Penal**. V 31. Ed. São Paulo: Atlas, 2015.

PAESANI, Liliana Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil**. São Paulo: Atlas, 2000.

O Direito na Sociedade da Informação III – A Evolução do Direito Digital. São Paulo: Atlas, 2013.

REALE, Miguel. **Noções Preliminares de Direito**. São Paulo: Saraiva, 2011

Redação Olhar Digital. **Qual a diferença entre hacker e cracker?**. Disponível em: <http://olhardigital.uou.com.br/fique_seguro/noticia/qual-a-diferenca-entre-hacker-e-cracker/38024>. Acesso em 28 de outubro de 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância. A privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SCHAFF, Adam. **A Sociedade Informática**. Traduzido por Carlos Eduardo J. Machado 4ª ed. São Paulo: Brasiliense, 1995.

SIMÃO FILHO, Adalberto. **Sociedade da informação e seu lineamento jurídico**. In: PAESANI, Liliana Minardi (Coord.). *Direito na sociedade da informação*. São Paulo: Atlas, 2007.

VAINZOF, Rony. **Da responsabilidade por danos decorrentes de conteúdo gerado por terceiros**. In: MASSO, Fabiano Del; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (Coords.). *Marco civil da internet: Lei 12.965/2014*. São Paulo: Revista dos Tribunais, 2014.

VELLOZO. Jean Pablo Barbosa. **Crimes Informáticos e criminalidade contemporânea**. Disponível em: <<http://jus.com.br/artigos/44400/crimes-informaticos-criminalidade-contemporanea/1>>. Acesso em 29 de outubro de 2019.

VIANNA, Túlio; MACHADO, Felipe. **Crimes Cibernéticos**. Belo Horizonte: Fórum, 2013.