Universidade
Estadual de Londrina

CENTRO DE ESTUDOS SOCIAIS APLICADOS
CURSO DE DIREITO
TRABALHO DE CONCLUSÃO DE CURSO

CRIMES CIBERNÉTICOS – A EFICÁCIA DA PUNIBILIDADE PELO PODER PÚBLICO À LUZ DA LEI 12.737/2012

Monique Elouise Lopes Geraldo

LONDRINA – PARANÁ

2016

MONIQUE ELOUISE LOPES GERALDO

CRIMES CIBERNÉTICOS – A EFICÁCIA DA PUNIBILIDADE PELO PODER PÚBLICO À LUZ DA LEI 12.737/2012

Trabalho apresentado como requisito para a Conclusão do Curso de Direito do Centro de Educação Sociais e Aplicados da Universidade Estadual de Londrina.

COMISSÃO EXAMINADORA

_____
Prof. Me. Benedicto de Souza Mello Neto
Universidade Estadual de Londrina

_____
Prof. Ms. Carlos José Cogo Milanez
Universidade Estadual de Londrina

_____
Mariana Moreno do Amaral
Universidade Estadual de Londrina

Londrina, 12 de julho de 2016

A meu pai José.

✡ 13.05.1949 – ✝ 09.09.2015.

AGRADECIMENTOS

Ao Prof. Ms. Orientador, tão paciente e encorajador para a realização deste trabalho, que não permitiu que transbordasse em desânimo e falta de foco.

Ao Prof. Ms. Fernando Perez, que aconselhou, deu suporte, material, e me guiou nessa jornada.

A minha família, pela confiança e por não cobrar resultados que não pudesse cumprir.

A meu pai que não está mais aqui mas tenho certeza que estou realizando também o seu sonho, e sei que apesar de tudo batalhou tanto para que visse chegar este momento.

Aos amigos, pelo apoio, compreensão, força e por mostrarem como basta dar o primeiro passo; que também emprestaram livros, leram e corrigiram.

Ao meu grande professor do Curso de Redação que não só me ensinou a escrever mas também a não colocar limite nisso e consequentemente ser mais crítica com o que nos cerca.

A meu professor de filosofia que tanto me inspirou.

Aos professores e colegas de Curso, pois juntos trilhamos mais essa etapa difícil, e tão importante em minha vida.

A todos que, com boa intenção, colaboraram para a realização e finalização deste trabalho.

Ao professor coordenador de TCC que incentivou a estudar mais para dar maior qualidade à minha monografia e consequentemente ao curso.

Aqueles que infelizmente não citei, talvez não tenham relação com o trabalho mas acima de qualquer coisa possuo grande apresso e contribuem para que eu seja o que sou.

E sobretudo à Deus, e toda e qualquer outra força que exista que me agraciou com todas as oportunidades que tive até hoje e assim permitiu que realizasse não só o meu sonho de entrar no curso de Direito da Universidade que sempre quis, como que o concluísse.

“Mais vale um jovem pobre e sábio do que um rei ancião e insensato, que em sua arrogância já não aceita mais conselhos”.

Eclesiastes 4.13

"O Lugar que o Homem deve ocupar e o papel que deve desempenhar no mundo dominado pelas maquinas".

Não há qualquer possibilidade do mundo vir a ser dominado por máquinas, graças à competência racional do homem. Se assim fosse, os animais teriam-no feito ao invés de simplesmente sobreviver diante das adversidades existentes desde o surgimento da Terra.

Mas, em um mundo repleto de máquinas, o homem possui um papel elementar capaz de destacá-lo; o de pensar e, um segundo, o de trabalhar. Ações que algumas máquinas podem exercer, porém devido à repetição e ao fato de existir alguém que a criou desta forma. Assim revela-se a superioridade da capacidade humana em relação à tecnologia.

O desenvolvimento desta ciência magnifica se dá graças ao homem. Com sua ausência, ela não existiria e tornaria impossível definí-la como boa ou má, uma vez que foi construída unicamente para servir, facilitar e auxiliar em seu cotidiano. Se em algum momento ela não o faz ou apresenta um destino voltado ao prejuízo dele, é porque há outro indivíduo capaz de errar que está em seu comando.

As máquinas atuam cada vez mais no dia-a-dia do homem, mas como mero instrumento passível de gerar a ele certo desconforto quando se depara temporariamente desprovido de certa tecnologia. Isto torna fundamental que ele não se permita dominar, iludir como papel desempenhado por ela, pois permanecerá capaz de executar qualquer atividade.

A tecnologia agiliza alguns processos e até mesmo toda uma produção, o que garantiu a origem dos objetos em série, mas não possibilidade de criar por si só um poema, uma manifestação de arte e quebrar os padrões existentes, dever do homem, que ultrapassa o fato de coabitar com ela, pois ele cria, imagina e pensa, o que tornar ridículo cogitar que a tecnologia por ele criada supere a ele a sua capacidade racional.

Constitui um erro que esse ser tão completo, dotado de habilidades únicas, as deixe de lado diante do comodismo proporcionado pela praticidade de objetos. Sua inteligência deve ser constantemente aperfeiçoada, posta para solucionar problemas enquanto a tecnologia exerce o papel de livrá-lo de realizar trabalhos repetitivos e até mesmo braçal.

Deste modo o papel do homem em uma sociedade repleta de máquinas é o de diferenciar-se, inovar, garantir o progresso dela através das suas competências e alcançar seus objetivos, e não esperar que a tecnologia a faça, impedindo-o de exercer seu livre-arbítrio e representando suas necessidades.

Monique Lopes – 2011

"Só quem não conhece o real significado –valor, razão de ser – do trabalho, da arte, da espiritualidade, teme as máquinas". Forte, Carlos

Geraldo Lopes, Monique Elouise. **Crimes Cibernéticos – A eficácia da punibilidade pelo Poder Público à Luz da Lei 12.737/2012.** 86 páginas. Trabalho de Conclusão de Curso. Curso de Direito. Centro de Estudos Sociais Aplicados da Universidade Estadual de Londrina, 2016.

RESUMO

O trabalho propõe-se a discutir o ambiente virtual, que com o avanço cada vez maior da tecnologia, se faz mais relevante e presente na sociedade moderna, tornando possível a realização de um grande número de atividades, especialmente sociais, de forma rápida, prática e no qual os indivíduos podem ser quem desejar ser, ou utilizarem de anonimato. É nesse contexto que se cria a noção de que tudo é possível dentro da Internet, sendo considerada por muitos uma terra sem leis e, portanto, propícia para atos de injúria, difamação, racismo, fraudes e crimes. Desmitificando a ideia de impunidade e enfatizando o impacto da Internet no Direito Penal, abre-se o debate acerca da legislação e da efetiva aplicação da justiça criminal dentro do mundo cibernético, de modo que este não interfira nos direitos dos usuários, como a liberdade de expressão.

Palavras-chave: Cibercrimes; Hacker; Direito Penal; Direito Digital; Eficácia.

Geraldo Lopes, Monique Elouise. **Cybernetic Crimes The Effectiveness of Punishment by The Public Power Under the Law 12.737/2012.** 86 pages. Trabalho de Conclusão de Curso. Curso de Direito. Centro de estudos sociais aplicados da Universidade Estadual de Londrina - UEL, 2016.

ABSTRACT

The written assignment proposes to discuss the web environment, which with the technology advance, becomes more relevant and present in the modern society, making possible the realization of a large number of activities, mainly social, in a quick and practice way, and which the individuals can be whoever they want to be, or even utilize an anonymous form. In this context, forms a notion that everything is possible on the Internet, even considered to be a land of no rules by many users and, therefore, propitious to acts of injury, defamation, racism, fraud and crimes. Demystifying the impunity idea and emphasizing the internet impact at the Criminal Law, opens up the debate about the legislation and the criminal justice effectiveness apply inside the cybernetic world, in a way that these don't interfere at the users rights, just like freedom expression.

Key Words: Cybercrimes; Hackers; Criminal Law; Digital Law; Efficiency

.

LISTA DE SIGLAS, ABREVIAÇÕES E SÍMBOLOS

RPANET	-	Advanced Research Projects Agency Network
art.	-	Artigo
Atual.		Atualizada
CC	-	Código Civil
Cit.	-	Citado(a)
CF	-	Constituição Federal da Republica Federativa do Brasil
CP	-	Código Penal Brasileiro
CPC	-	Código de Processo Civil
CPP	-	Código de Processo Penal
Coord.	-	Coordenador(a)
Ed.	-	Edição
IP	-	Internet Protocol
Kbp	-	kilobytes
MIT	-	Massachuts 13nstituto f Technology
MC	-	Marco Civil
n.	-	Número
Org.	-	Organizador
s/d	-	Sem data
Trad.	-	Tradução
TPC/IP	-	Transmission Control Protocol/ Internet Protocol
Vol.	-	Volume
WWW	-	World Wide Web

SUMÁRIO

1 INTRODUÇÃO 12

2 DA INTERNET 15

2.1 CONSIDERAÇÕES PRELIMINARES 15

2.2 CONCEITO 17

2.3 EVOLUÇÃO HISTÓRICA 20

2.4 O ACESSO À INTERNET COMO DIREITO FUNDAMENTAL 26

3 DOS CRIMES CIBERNÉTICOS 30

3.1 CONCEITO 30

3.2 HISTÓRICO 32

3.3 TIPIFICAÇÃO PENAL 39

3.4 ASPECTOS DOGMÁTICOS 41

4 DOS CRIMES DE ACESSO NÃO AUTORIZADO A SISTEMA INFORMÁTICO – ART.154-A 46

4.1 CONSIDERAÇÕES PRELIMINARES 46

4.2 BEM JURÍDICO PROTEGIDO 47

4.3 SUJEITO DO DELITO 48

4.4 TIPICIDADE OBJETIVA 53

4.5 TIPICIDADE SUBJETIVA 54

4.6 CONSUMAÇÃO E TENTATIVA 56

4.7 SANÇÃO PENAL E ASPECTOS PROCESSUAIS PENAIS 58

5 CONSIDERAÇÕES FINAIS 60

6 REFERÊNCIAS 63

ANEXOS 66
Anexo I - Jurisprudências.....67
Anexo II - LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.....70
Anexo III - LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.....72
Anexo IV - LEI Nº 12.965, DE 23 DE ABRIL DE 2014.....75

1 INTRODUÇÃO

O presente trabalho de conclusão de curso se ampara na grande relevância que o tema possui para humanidade, uma vez que o avanço tecnológico acontece sem qualquer limite e, ainda que seja de grande contribuição para o desenvolvimento sociocultural, acaba por impactar diretamente no Direito Penal, afinal, surgem usuários que utilizam desse progresso para cometer atos ilícitos.

No entanto, não é possível alterar as normas a cada novo passo da ciência, novo progresso da Internet, ou mudar as normas a cada nova tecnologia, e ainda que o fizesse, até que uma lei entrasse em vigor haveria grandes chances de que esta já caminhasse para a obsolescência.

No caso do Brasil, são inúmeras as ocorrências e delitos, desde fraudes no comércio eletrônico, crimes de injúria, difamação e racismo à crimes sexuais. Isso acontece porque o agente destas infrações são encorajados por se valer-se da Internet – um ambiente onde há o sentimento de impunidade e anonimato, no qual parece ser mais fácil cometer tais delitos – espaço este em que se tem a comodidade e a praticidade de poder cometer delitos sem passar por riscos, exposição, e sequer ter que sair de casa. Além claro, de que são inúmeras as prováveis vítimas. Afinal, não é necessário se deslocar a procura daquela que parece mais vulnerável, ou mesmo mais atrativa, já que são superadas tais barreiras espaciais.

Sem muito rigor, é como imaginar um assaltante que do conforto da janela de sua casa vê passar inúmeras pessoas a quem possa abordar, existindo um grupo vulnerável e/ou que possuam mais objetos que chamem sua atenção.

Tal situação se agrava ao pensar que o ciberespaço[1] não possui qualquer regulamentação específica e as poucas que tipificam condutas cometidas nele despontaram ao longo dos anos de 2012 e 2014, quando inúmeros casos públicos pressionaram a entrada em vigor da Lei 12.737/2012, 12.735/2012 e do Marco Civil da Internet (Lei 12.965/14). Até esse momento os crimes perpetrados nesta esfera eram amparados pela lei comum, mediante a existência de um resultado posterior.

[1] William Gibson define o ciberespaço como um espaço não físico ou territorial, que se compõe de um conjunto de redes de computadores, por meio das quais todas as informações circulam. http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html

Portanto, o objetivo deste trabalho é questionar se existe uma punição para agentes de condutas ilícitas relacionadas aos dispositivos informáticos e a Internet. Uma vez que exista punição, ela se faz eficaz? É capaz de inibir a prática desses crimes? E se cometidos, possuirá o poder de reparação?

Essas leis são responsáveis por regular as relações e atividades desenvolvidas na rede mundial de computadores; bem como pune condutas típicas recém-criadas, igual o caso dos artigos 154-A e 154-B do Código Penal.

Desta forma é provável que futuramente essas leis não abrangerão todos os bens jurídicos necessários, inclusive porque a rede nada mais é que uma extensão do dia-a-dia do homem, e inevitavelmente se tornará ainda mais essencial e dinâmica. Assim, é imprescindível o entendimento dessa legislação para receber o futuro a fim de proteger a intimidade, privacidade, segurança econômico-financeira dos cidadãos.

Consoante a isso é necessária à discussão a cerca da plena aplicação da justiça criminal, da garantia e proteção aos bens jurídicos, inclusive daqueles que ainda não foram tutelados nesta lei, para que haja a promoção da manutenção paz social.

A metodologia utilizada foi um estudo exploratório e pesquisa bibliográfica numa revisão de literatura que permitiu edificar conceitos teóricos, métodos e instrumentos de análise, através de referências bibliográficas ou citações de artigos, trabalhos e aplicações semelhantes em outros contextos, revistas, dissertações, publicações referentes ao objeto da investigação e mídia eletrônica, em material publicado em livros, revistas e jornais, podendo ser feita em fonte primária ou secundária.

A pesquisa bibliográfica procura explicar um problema a partir de referências teóricas publicadas (em livros, revistas). A pesquisa visa descrever uma determinada realidade, logo pode ser considerada como descritiva, do tipo teórico e empírico. No presente trabalho serão realizadas revisão e interpretação dos estudos pertinentes, implicando na seleção, leitura e análise de conceitos que abrangem o tema, permitindo assim, maior clareza nos dados e na formulação de comparações com aplicações práticas.

Portanto, este trabalho está dividido em quatro capítulos:

No primeiro capítulo relata-se sobre a internet fazendo as considerações preliminares, assim como conceito; a evolução histórica, dando ênfase ao acesso a

internet como direito fundamental e as tendências evolutivas. No segundo capítulo aborda-se sobre os crimes cibernéticos seus significados e históricos a tipificação penal e os aspectos dogmáticos.

Na sequência no terceiro capítulo assevera-se as considerações preliminares sobre os crimes de acesso não autorizado a sistema informático conforme art.154-a, no qual mostra o bem jurídico protegido, enfatizando o sujeito do delito, a tipicidade objetiva, a tipicidade subjetiva, a consumação e tentativa, a sanção penal e aspectos processuais penais.

Por fim, na última seção, figura as considerações finais da pesquisa, resumindo os resultados, expondo as conclusões obtidas por meio da análise dos dados e das obras pesquisadas, e ressaltando a eficácia da punibilidade pelo poder público à luz da Lei 12.737/2012 nos Crimes Cibernéticos.

2 DA INTERNET

2.1 CONSIDERAÇÕES PRELIMINARES

Conforme expõe Rogério Greco[2], “vivemos novos tempos e devemos nos adaptar, consequentemente, ao mau uso de todo esse aparato tecnológico”. Ou seja, diante dessa sociedade a cada passo mais dinâmica e integrada, contemplada pelos grandes avanços científicos e tecnológicos faz se necessário ter consciência que a ferramenta não é algo maléfico, não produz efeitos por si; pelo contrário, toda tecnologia é e sempre será positiva, quem concede um mau uso à ela é o próprio homem; relembramos assim Thomas Hobbes, que já enfatizava que o homem é o lobo do homem. O que em outras palavras foi ratificado pelo psicólogo americano Burrhus Frederic Skinner[3]:

> Talvez não seja a ciência que está errada, mas sua aplicação. Os métodos da ciência têm tido um sucesso enorme onde quer que tenham sido experimentados. Apliquemo-los, então, aos assuntos humanos. Não precisamos nos retirar dos setores onde a ciência já avançou. É necessário apenas levar nossa compreensão da natureza humana até o mesmo grau.

Ao aplicar isso à atualidade, é possível ver com clareza que o que determina os efeitos da tecnologia é quem a utiliza. Este é o momento decisivo, o ponto de interferência do homem, cujo papel pode ser classificado como bom, como produtor dos avanços mais fantásticos, como pesquisador, solucionador de problemas e capaz de justificar sua existência com qualidade e sabedoria; versus aquele que também é hábil, porém legalmente inadequado ou que contém potencial lesivo.

Enquanto esta tecnologia estava a favor exclusivamente de estudiosos, inquiria-se a evolução, e portanto não havia relatos de um mau comportamento. Bastou ganhar público para que a sua finalidade fosse transformada. Exatamente o que aponta a autora Rita de Cássia Lopes da Silva[4]:

---

[2] GRECO, Rogério. GRECO, Rogério. **Curso de Direito Penal: parte especial**, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa - 11 . ed. Niterói, RJ: Impetus, 2015.p. 600.

[3] SKINNER, Burrhus Frederic, 1904-1990. **Ciência e comportamento humano /** B. F. S kinner; tradução João Carlos Todorov, Rodolfo Azzi. 1a ed. - São Paulo: Martins Fontes, 2003. - (Coleção biblioteca universal), p.5.

[4] SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informático**. São Paulo: Editora Revista dos Tribunais, 2003, p.19.

> Durante toda a tecnológica de um equipamento que facilitasse os cálculos matemáticos, não houve notícias de que o homem tivesse agido de forma a lesionar ou pôr em perigo de lesão qualquer bem jurídico na utilização desses equipamentos em evolução. Vale dizer que as máquinas construídas não foram utilizadas como meios para qualquer prática delitiva, mesmo porque eram de uso exclusivo de pesquisadores que tinham como meta única o aperfeiçoamento dos equipamentos e a obtenção de resultados rápidos e confiáveis que viessem a facilitar o trabalho dos pensadores. Os problemas decorrentes do uso ilícito do equipamento eletrônico somente surgiram quando passaram a fazer parte do cotidiano da população; quando saíram da esfera de utilização exclusiva da pesquisa cientifica para tornarem-se um equipamento de uso comum.

Por oportuno, a Internet dá forças e até mesmo coragem para que o indivíduo pratique seus delitos. Os cibercriminosos colocaram a tecnologia a seu favor e viram sua conduta ilegal potencializada, já que com ela o sentimento de garantia do anonimato fora majorada. Consorte, uma vez bem treinado esse indivíduo facilmente conseguirá andar por esse mundo sem deixar rastros, sem expor seu rosto, vida e hábitos.

Ajustado a isso, existe outro empecilho, a característica peculiar, a fragilidade dos sistemas informatizados frente aos convencionais, graças à sua modalidade de armazenagem, a qual pode ser acessada a qualquer tempo e de qualquer lugar, de modo a viabilizar estas condutas inadequadas.

Rita de Cássia Lopes da Silva[5] aponta que este "sistema é vulnerável, está sujeitos a erros, mau uso e ao crime, pois apresenta a armazenagem de dados na forma eletrônica, o que propícia a facilidade de acesso, alterações e destruição".

Nesse norte, Iso Chaitz Scherkerkewitz[6] também aborda a fragilidade deste meio e a falta de proteção ao citar as formas de comunicação e interação que a Internet nos oferece:

> É logico que cada uma dessas formas de comunicações possui características próprias, porém, o que congrega todas essas formas de comunicação é o meio usado para a transmissão de informações (a Rede – o conexo de computadores) e a necessidade de proteção às informações trocadas.

Desta forma, existe um local propício para a adoção de condutas inadequadas, mas segundo Túlio Vianna e Felipe Machado[7] não quer dizer que todo ato ali praticado configurará um crime informático:

---

[5] SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informático.** São Paulo: Editora Revista dos Tribunais, 2003, p.36.
[6] SCHERKERKEWITZ, Iso Chaitz. **Direito e Internet**. São Paulo: Editora Revista dos Tribunais, 2014, p.22.
[7] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Forum, 2013; p.29.

> A simples utilização pelo agente de um computador para execução de um delito, por si só, não configuraria um crime informático, caso o direito afetado não seja a informação automatizada. Ocorre, no entanto, que muitos autores acabaram, por analogia, denominando como crimes informático as infrações penais em que o computador serviu como mero instrumento utilizado na prática do delito. Apesar de imprópria, esta denominação se tornou muito popular e hoje é impossível ignorá-la.

É importante a compreensão deste universo, da postura de seus usuários e se há uma adequação com o ordenamento jurídico brasileiro. Quais são os direitos, o que se protege, porque é protegido. Qual é a correta definição, e a nomenclatura aconselhada. A despeito disso qual a adequada punição aos agentes destas condutas, se são todas verdadeiramente ilícitas, ou mesmo que desonestas são moralmente aceitas? Por conseguinte, esta punição é eficaz? Ela coíbe a prática destes comportamentos?

2.2 CONCEITO

A Internet, também conhecida como Rede, é composta a partir da conexão de vários computadores que compartilham informações entre si e ainda disponibilizam serviços por todo o planeta.

Com a publicação da Lei 12.965, de 23.04.2014, o art. 5°, I, a define como: "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;[8]"

Afinado a isso, para o autor Iso Chaitz Scherkerkewitz[9], que cita Guilherme Magalhaes Martins, a definição de Internet é:

> A Internet (International Network of Computers) é constituída por uma rede de computadores que estão conectados por linhas telefônicas, fibras óticas, cabos submarinos, satélites, etc. E vinculam Universidades, Governos, empresas e milhões de pessoas, independentemente de fronteiras geográficas. Uma definição mais técnica de Internet é dada por Guilherme Magalhaes Martins, no sentido de ser "uma rede aberta decorrente da conexão de várias redes entre si, perfazendo-se a comunicação por meio de um conjunto de protocolos, denominados Transmission Control Protocol/Internet Protocol (TCP/IP)[10].

---

[8] Art. 5°, I, da Lei n.º 12.965 de 23 de Abril de 2014.
[9] SCHERKERKEWITZ, Iso Chaitz. **Direito e Internet.** São Paulo: Editora Revista dos Tribunais, 2014, p. 14.
[2] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet.** São Paulo: Ed. RT, 2008.p.30.

Muito similar à ideia exposta por Túlio Vianna e Felipe Machado[11]:

> A Internet é uma rede global que consiste na interconexão de inúmeras redes que usam o mesmo protocolo[12]. Logo, ela permite interligar sistemas informáticos de todo o planeta, proporcionando o recebimento e o envio de informações.

Adiante na conceituação, é imprescindível esclarecer que este aglomerado de computadores não possui um órgão gerenciador, não se subordina, por exemplo, a um país ou conjunto de líderes/membros. Problematização essa, contemplada pela autora Rita de Cássia Lopes da Silva:

> Não há um único centro que governa ou mesmo gerencia a internet. As redes constituintes pertencem a alguma organização, mas ela não é de ninguém. Quando se fala em decisões sobre a internet, sendo estas apenas em padrões tecnológicos, elas são de responsabilidade de órgãos como a Internet Numbers Authority, a Internet Engineering Task Force e a Isoc, que é uma organização de membros voluntários conhecida como Internet Society, tendo como membro qualquer pessoa ou organização que apresentar interesse em aderir a ela.

E independente do conceito que possa ser atribuído à internet, ou ainda como se dá seu gerenciamento, a beleza desta está na redução de fronteiras, na aproximação dos povos, na quebra da limitação do tempo e sobretudo na revolução do conhecimento; está no fato de cunhar inúmeras possibilidades que antes não poderiam ser imaginadas ou esperadas, sendo portanto inegável seus inúmeros benefícios, e a origem de um sistema que conecte tudo e de todos.

Tão capaz de resguardar todas as áreas, que possibilitou que os mercados se expandissem; que a economia de um país agora atinja a de outro com proporções mais intensas; a existência da comunicação com zonas remotas ou sob influência da censura, ainda que indiretamente.

A cultura se alastrou, os mais diversos produtos se tornaram acessíveis, e até a moda mais sofisticada, agora atinge vários povos e é produzida para ser difundida e adquirida por todos os continentes.

Iso Chaitz Scherkerkewitz[13] aponta para isso como reflexo da massificação. “Não apenas intelectuais tiveram acesso a Rede, mas esta ficou aberta a todas as

---

[11] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos.** Belo Horizonte: Forum, 2013, p. 24.
[12] Agrupamento de regras que regulam a transmissão de dados entre computadores.
[13] SCHERKERKEWITZ, Iso Chaitz. **Direito e Internet.** São Paulo: Editora Revista dos Tribunais, 2014, p. 16.

camadas da sociedade, inclusive as mais populares e com menor cultura."

É praticamente impossível que algo não seja difundido pela Rede, que se da sobretudo com uma velocidade assustadora e passou a ser desejado por todos. Citando ainda o mestre da PUC:[14]

> O mundo ficou menor com o avanço da tecnologia. As distâncias físicas fora, rapidamente superadas, como nunca havia sido sequer sonhado. O comércio ficou globalizado. O conhecimento foi compartilhado em uma escala jamais vista (os centros produtores de conhecimento conseguiram criar conjuntamente, os avanços da medicina puderam ser compartilhados – a telemedicina é uma realidade que comprova a nossa afirmação).

Diante disso se torna nítida a repetição histórica; o que ocorreu com o avanço das grandes navegações, com o surgimento dos telegramas, da telefonia e a Revolução Industrial, acontece agora com a Internet. Como aborda Spencer Toth Sydow[15]:

> De tempos em tempos, a sociedade sofre evoluções que a transformam. Assim foi com as Revoluções Burguesas, mais especificamente a Revolução Francesa, que por conta do questionamento, trouxe o inicio da positivação de direitos fundamentais. Assim foi a Revolução Industrial que, por conta dos avanços tecnológicos, trouxe a substituição das ferramentas pelas máquinas, consolidando o capitalismo como modo de produção (...)
> Em tempos recentes surgiu uma nova Revolução, por nos denominada Revolução Digital.
> Entende-se por Revolução Digital o movimento de inserção na sociedade de novas tecnologias e serviços que utilizam desenvolvimentos recentes e que modificam a forma como o cotidiano cidadão progride.

Tudo o que conhecemos será submetido à Internet e outras formas de tecnologia; são novas formas de comunicações, novos mecanismo de obtenção de provas e de confecção de contratos. Tão logo o direito todo não só terá seu apoio e utilizará de suas ferramentas como também deverá ser englobado por ela. Mas é necessário lembrar que, como afirma Spence Toth Sydow[16], "grandes desenvolvimentos trazem consigo novas responsabilidades e riscos".

Hoje a aplicação do Código Penal é válida e suficiente, mas é inquestionável que necessita de amparo para suprir tal demanda, afinal seu princípio basilar é a adequação e tipificação penal, mas com a velocidade que a

---

[14] Ibid. p. 19-20.
[15] SYDOW, Spencer Toth. **Crimes Informáticos e suas vítimas**. 2ed. – São Paulo: Saraiva, 2015, p. 19.
[16] Ibid, p. 20.

sociedade caminha, logo haverá ações que não estarão comtempladas.

Um exemplo disso são as "Lei Carolina Dieckmann[17]" e o Marco Civil, ainda que extremamente recentes, controversas em alguns aspectos; o segundo em especial, capaz de permitir mais de uma interpretação; deixaram pontos obscuros, e diversas lacunas, mas ainda assim conseguiram abranger casos, até então sem previsão legal.

Verifica-se isso no texto de Iso Chaitz Scherkerwitz[18]: "Infelizmente o mundo jurídico ainda não possui uma uniformidade de regras aplicáveis, o que acaba, diante da globalização, gerando grandes dúvidas na solução dos problemas apresentados por essa nova realidade."

Diante da evolução do conhecimento humano é necessário fomentar tal discussão a fim de que promova-se com efetividade a garantia dos bens jurídicos que serão apresentados.

2.3 EVOLUÇÃO HISTÓRICA

É de conhecimento comum à origem do computador e da Internet. Ambos nasceram com o intuito de servir ao militarismo e a guerra; não só o fizeram como foram também determinante em seu resultado.

Os primeiros e enormes computadores despontaram na Segunda Guerra Mundial, enquanto que a Internet raiou na década de 60, nos Estados Unidos, com a Guerra Fria, para facilitar o "intercâmbio de informações descentralizadas"[19].

No entanto, frise-se que para a autora Rita de Cássia, citando João Carlos Kanaan[20] "a história do desenvolvimento da informática se iniciou, verdadeiramente, a partir da criação do conceito de armazenamento das informações".

Acrescente-se, que esse era o desejo do homem, literalmente desde a idade da pedra, quando se valiam de pedras, gravetos, e todo e qualquer artifício, para realizar a marcação, ou retratar os fatos de sua época.

Mais além, durante o período Mesopotâmio, ascende o ábaco a fim de

---

[17] Lei n. °12.737 de 30 de Novembro de 2012 ("Lei Carolina Dieckmann")
[18] SCHERKERKEWITZ, Iso Chaitz. Direito e Internet. São Paulo: Editora Revista dos Tribunais, 2014, p. 21.
[19] TAKAHASHI, Tadao (Org.). Sociedade da Informação no Brasil: Livro verde. Brasília. Ministério da Ciência e Tecnologia, 2000. p. 133.
[20] KANAAN, João Carlos. **Informática global:** tudo o que você precisa saber sobre informática. São Paulo: Pioneira, 1998. p.24

agilizar os cálculos, e pela mesma motivação, no final só século XIX, nos Estados Unidos cria-se uma máquina para acelerar os cálculos com o censo do país.

Ao analisar o pensamento de Rogério Greco[21] conclui-se que apesar desta abissal necessidade, infelizmente o destaque viria apenas após o uso militar, quando essa tecnologia remanescente despertou a curiosidade de empresas e ganhou uma roupagem mais amigável e simplificada para promover as interações; como o modelo World Wide Web – WWW, o qual resultaria nos futuros provedores de acesso e na conexão particular à Rede.

> Originalmente, a internet teve uma utilização militar, sendo que a ideia de uma rede interligada surgiu em 1962, durante a Guerra Fria, e foi imagina, conforme esclarece Augusto Rossini, "para proteger a rede de computadores do governo norte-americano após um ataque nuclear. Planos detalhados foram apresentados em 1976, tendo sido criada a Arpanet[22] em 1968, estabelecendo-se o germe do que é hoje internet" concebida, entre outros, por Paul Baran, da empresa Rand Corporation, também com a finalidade de suprir as deficiências e meio de comunicação cientifica interuniversitaria.

Já no Brasil a Internet possui pouco mais de duas décadas, e ainda assim não teve um objetivo distinto da estadunidense; sua evolução foi célere, primeiramente foi introduzida unicamente nos meios acadêmicos. Aproximadamente cinco anos mais tarde, o governo permitiu sua abertura, de modo experimental, para só depois ganhar a população. Como descreve o nobre jurista Emanuel Sperandio Gimenes[23]:

> A história da Internet no Brasil começou bem mais tarde, só em 1991, com a RNP (Rede Nacional de Pesquisa), uma operação acadêmica subordinada ao MCT (Ministério de Ciência e Tecnologia).
> Em 1991, a RNP (Rede Nacional de Pesquisas) trouxe a Internet para o Brasil, sendo o seu objetivo o de atender à conexão das redes de universidades e centros de pesquisas, mas logo as esferas federal e estadual começaram também a se interligar. Em 1994, no dia 20 de dezembro, a Embratel lançou o serviço experimental a fim de conhecer melhor a Internet. Em 1995, finalmente, os Ministérios de Comunicações e de Ciência e Tecnologia abriram a Internet para operação comercial, e os provedores puderam contratar conexões com a RNP e, depois, com a Embratel. Enfim, houve a abertura ao setor privado da Internet para exploração comercial da população brasileira. A RNP ficou responsável pela infraestrutura básica de interconexão e informação em nível nacional, tendo controle do backbone[24].

Atualmente, o Brasil possui diversos backbones interligando todos os

---

[21] GRECO, Rogério. **Curso de Direito Penal:** parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa. 11. ed. Niterói, RJ: Impetus, 2015, p. 600.
[22] ARPANET – primeira rede operacional de computadores à base de comutação de pacotes.
[23] http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html
[24] Backbone: Coluna dorsal de uma rede representa a via principal de informações transferidas por uma rede, neste caso, a Internet.

Estados do país, bem como centenas de conexões com outros países. A evolução em número de usuários coaduna com os dados apresentados por Iso Chaitz Scherkerkewitz[25].

Neles é crescente o número de usuários da Internet. Ao comparar o Brasil, nas datas de 30.06.2012 e 30.11.2015, pode ser interpretado que antes sua posição entre os 20 países com o maior número de internautas saltou de 5° para 4° lugar no ranking; ou seja, haviam 193,946,886 usuários, passando para 204,259,812.

TOP 20 PAÍSES COM MAIS USUÁRIOS DE INTERNET – JUNHO 2012

#	País ou Região	População estimada 2012	Usuários da Internet Ano 2000	Usuários da Internet (Última pesquisa)	Penetração (% População)	Users % World
1	China	1,343,239,923	22,500,000	538,000,000	40.1 %	22.4 %
2	United States	313,847,465	95,354,000	245,203,319	78.1 %	10.2 %
3	India	1,205,073,612	5,000,000	137,000,000	11.4 %	5.7 %
4	Japan	127,368,088	47,080,000	101,228,736	79.5 %	4.2 %
5	Brazil	193,946,886	5,000,000	88,494,756	45.6 %	3.7 %
6	Russia	142,517,670	3,100,000	67,982,547	47.7 %	2.8 %
7	Germany	81,305,856	24,000,000	67,483,860	83.0 %	2.8 %
8	Indonesia	248,645,008	2,000,000	55,000,000	22.1 %	2.3 %
9	United Kingdom	63,047,162	15,400,000	52,731,209	83.6 %	2.2 %
10	France	65,630,692	8,500,000	52,228,905	79.6 %	2.2 %
11	Nigeria	170,123,740	200,000	48,366,179	28.4 %	2.0 %
12	Mexico	114,975,406	2,712,400	42,000,000	36.5 %	1.7 %
13	Iran	78,868,711	250,000	42,000,000	53.3 %	1.7 %
14	Korea	48,860,500	19,040,000	40,329,660	82.5 %	1.7 %
15	Turkey	79,749,461	2,000,000	36,455,000	45.7 %	1.5 %
16	Italy	61,261,254	13,200,000	35,800,000	58.4 %	1.5 %
17	Philippines	103,775,002	2,000,000	33,600,000	32.4 %	1.4 %
18	Spain	47,042,984	5,387,800	31,606,233	67.2 %	1.3 %
19	Vietnam	91,519,289	200,000	31,034,900	33.9 %	1.3 %
20	Egypt	83,688,164	450,000	29,809,724	35.6 %	1.2 %
TOP 20 Countries		4,664,486,873	273,374,200	1,776,355,028	38.1 %	73.8 %
Rest of the World		2,353,360,049	87,611,292	629,163,348	26.7 %	26.2 %
Total World Users		7,017,846,922	360,985,492	2,405,518,376	34.3 %	100.0 %

NOTES: (1) Top 20 Internet User Statistics – atualizado até 30 de junho de 2012.
www.e-commerce.org.br Fonte: www.internetworldstats.com e institutos diversos

Fonte: SCHERKERKEWITZ, 2014, p.28-29

[25] SCHERKERKEWITZ, Iso Chaitz. Direito e Internet. São Paulo: Editora Revista dos Tribunais, 2014, p. 28-29

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - NOVEMBER 30, 2015						
#	Country or Region	Population, 2015 Est	Internet Users Year 2000	Internet Users 30 Nov 2015	Penetration (% Population)	% Growth 2000 - 2015
1	China	1,361,512,535	22,500,000	674,000,000	49.5 %	2,895.6 %
2	India	1,251,695,584	5,000,000	375,000,000	30.0 %	7,400.0 %
3	United States	321,368,864	95,354,000	280,742,532	87.4 %	194.4 %
4	Brazil	204,259,812	5,000,000	117,653,652	57.6 %	2,253.1 %
5	Japan	126,919,659	47,080,000	114,963,827	90.6 %	144.2 %
6	Russia	146,267,288	3,100,000	103,147,691	70.5 %	3,227.3 %
7	Nigeria	181,562,056	200,000	92,699,924	51.1 %	46,250.0 %
8	Indonesia	255,993,674	2,000,000	78,000,000	30.5 %	3,800.0 %
9	Germany	81,174,000	24,000,000	71,727,551	88.4 %	198.9 %
10	Mexico	121,736,809	2,712,400	60,000,000	49.3 %	2,112.1 %
11	United Kingdom	64,767,115	15,400,000	59,333,154	91.6 %	285.3 %
12	France	66,132,169	8,500,000	55,429,382	83.8 %	552.1 %
13	Bangladesh	168,957,745	100,000	53,941,000	31.9 %	53,841.0 %
14	Egypt	88,487,396	450,000	48,300,000	54.6 %	10,633.3 %
15	Vietnam	94,348,835	200,000	47,300,000	50.1 %	23,550.0 %
16	Philippines	109,615,913	2,000,000	47,134,843	43.0 %	2,256.7 %
17	Iran	81,824,270	250,000	46,800,000	57.2 %	18,620.0 %
18	Turkey	77,695,904	2,000,000	46,282,850	59.6 %	2,214.1 %
19	Korea	49,115,196	19,040,000	45,314,248	92.3 %	138.0 %
20	Thailand	67,976,405	2,300,000	38,000,000	55.9 %	1,552.2 %
TOP 20 Countries		4,921,411,229	257,186,400	2,455,770,654	49.9 %	854.9 %
Rest of the World		2,338,491,014	103,799,092	910,490,502	38.9 %	777.2 %
Total World Users		7,259,902,243	360,985,492	3,366,261,156	46.4 %	832.5 %

NOTES: (1) Top 20 Internet User Statistics were updated for November 30, 2015. (2) Additional data for individual countries and regions may be found by clicking each country name. (3) The most recent user information comes from data published by Nielsen Online, International Telecommunications Union, Official country reports, and other trustworthy research sources. (4) Data from this site may be cited, giving the due credit and establishing an active link back to www.internetworldstats.com. Copyright © 2016, Miniwatts Marketing Group. All rights reserved worldwide.

Fonte: **http://www.internetworldstats.com/top20.htm**

Frente a esses dados é difícil vislumbrar que a princípio a Internet era discada e não chegava a 56kbp, realidade assustadoramente distante da atualidade, na qual o país é o quarto em número de usuários no mundo, figura entre os dez[26] maiores produtores mundiais de *vírus* e programas nocivos e com alta concentração de hackers. Como pode ser acompanhado na notícia do Grupo UOL[27] que divulgou o resultado feito pela empresa Symantec:

> Brasil é um dos 10 países onde mais surgem vírus de computador.

[26] http://www.istoedinheiro.com.br/blogs-e-colunas/post/20160506/brasil-grande-produtor-virus/8824. Acesso 12.06.2016 as 18h07.

[27] http://olhardigital.uol.com.br/fique_seguro/noticia/brasil-e-um-dos-10-paises-onde-mais-surgem-virus-de-computador/57806 .> Acesso em 30.04.2016 as 16h58.

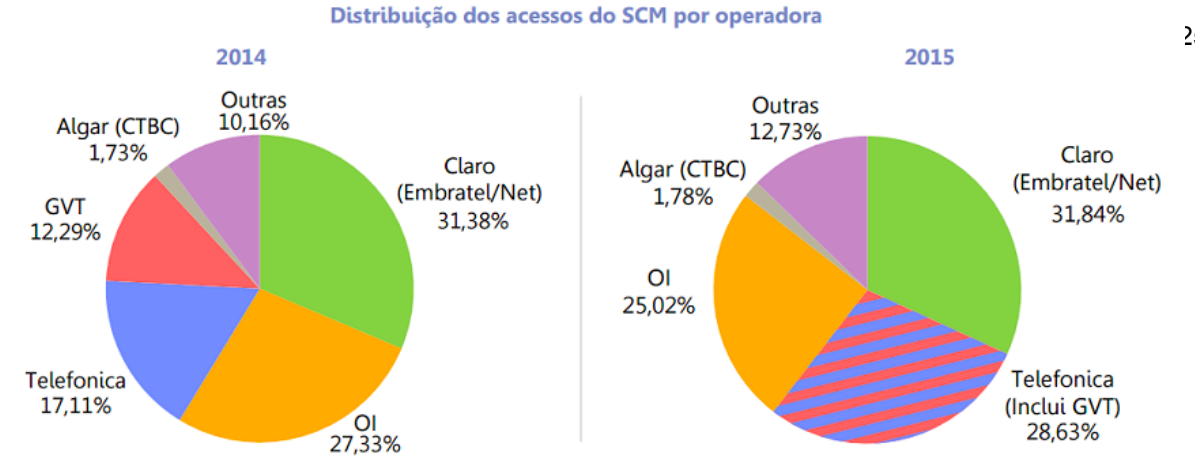
> REDAÇÃO OLHAR DIGITAL 29/04/2016 18H03 BRASIL MALWARE SEGURANÇA. A empresa de segurança em tecnologia Symantec divulgou nesta sexta-feira, 29, seu tradicional relatório anual de ameaças à segurança na internet. Entre os dados levantados, descobriu-se que o Brasil é um dos 10 países no mundo de onde mais nascem vírus de computador. Só na América Latina, o Brasil ocupa o primeiro lugar no ranking de países que mais "exportam" malware para o mundo, à frente de México e Argentina. Na lista global, os campeões são China, Estados Unidos e Índia. Curiosamente, porém, o Brasil também é um dos países mais atacados por ramsonware (vírus que "sequestra" dados da vítima em troca do pagamento de um resgate). Mais de 71% do total das contaminações por vírus de computador no Brasil se dá por meio de posts compartilhados manualmente em redes sociais, como o Facebook. É o maior índice da América Latina, enquanto os países vizinhos são mais vítimas de ofertas falsas de prêmios ou promoções: mais de 80% na Colômbia, 70% na Argentina e Peru, e 51% no México. O relatório também afirma que cerca de 500 milhões de dados pessoais foram roubados ou perdidos em todo o mundo ao longo de 2015. Mais detalhes sobre o estudo da Symantec (...). Grifo nosso.

E para Damásio de Jesus[28] a rapidez dessa evolução é fruto sobretudo, da economia:

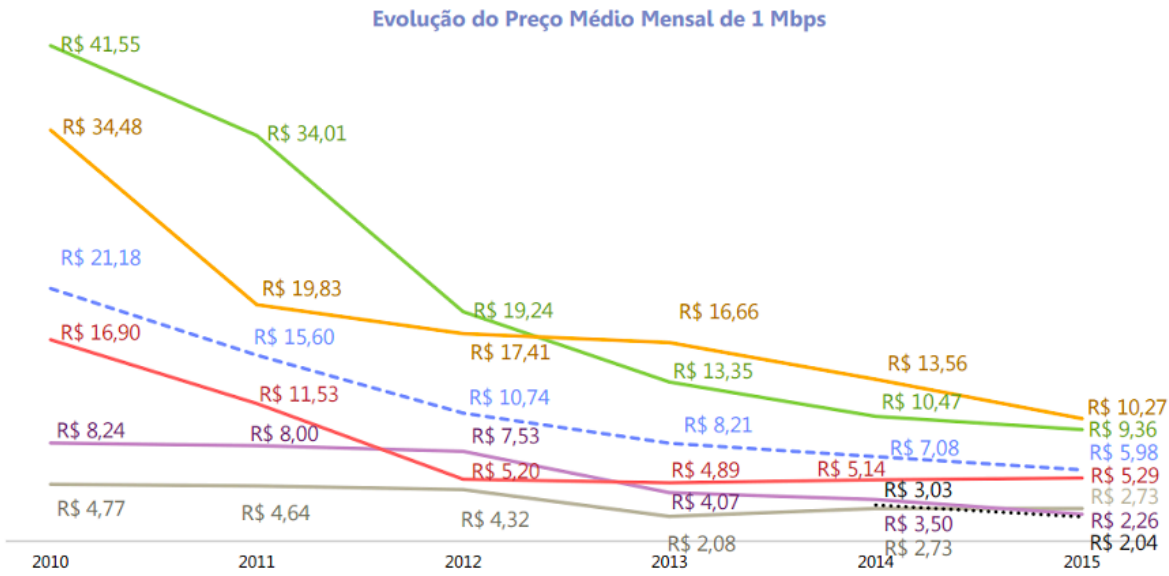
> A convergência tecnológica, a dinâmica industrial e a queda dos preços dos equipamentos, aliados ao vertiginoso crescimento da Internet, são as molas propulsoras das recentes transformações sociais locais. O Brasil, ultrapassa pela primeira vez 100 milhões de usuários da Internet. A evolução foi rápida, eis que duas décadas atrás utilizávamos redes Fidonet, conectando-se com pessoas através de BBS's (Bulleting Board Systems) e modens que nos permitiriam o acesso discado, muitas vezes em não mais de 56 kbp (kilobytes por segundo).

Ou seja, houve o aumento no número de empresas que oferecem o serviço e consequentemente a competição entre elas, de modo a reduzir os valores repassados para os cliente como pode ser visto nos gráficos abaixo:

[28] JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 13.



Via Anatel



Segundo pesquisa da Anatel[29] o custo da internet caiu 70% nos últimos 5 anos, mais uma razão pela qual a Internet no Brasil tenha evoluído significativamente e tão rápida.

Com alto número de usuários, preferência dada à esta frente a televisão, facilidade de comunicação e ainda seu barateamento propiciaram que o comportamento do brasileiro se alterasse, o acesso a outros conteúdos e mais tarde a popularização de condutas ilícitas, ainda que moralmente aceitas, como downloads indevidos e a pirataria.

[29] http://olhardigital.uol.com.br/noticia/preco-da-internet-fixa-brasileira-caiu-mais-de-70-em-5-anos/59518. Acesso em 20.06.16 as 21h10

2.4 O ACESSO À INTERNET COMO DIREITO FUNDAMENTAL

O papel da Internet é tão importante na atualidade que a ONU busca o reconhecimento do acesso à Internet como Direito Fundamental, pois ela junto as outras formas de comunicação básica e de promoção dos serviços de informação, se tornou primordial para garantir aos cidadãos o exercício pleno do direito à informação, da liberdade de expressão e possibilitou a globalização da cultura e educação.

O acolhimento deste conceito só é possível no Brasil graças à cláusula de abertura a Tratados e Conversões Internacionais presente no artigo 5°, §2° da Constituição Federal (CF):

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.[30] (grifo nosso).

O que é ratificado pelo autor Spencer Toth Sydow,[31] o qual entende o reconhecimento da Internet como direito difuso e universal para o Estado brasileiro:

> (...) conclui-se que o Brasil nitidamente quer entender o direito à internet como sendo difuso e universal, ao dizer, em seu art. 4°, I, que o acesso à internet é direito de todos.
> O art. 5° demonstra claramente que há uma compreensão do fenômeno sociológico da rede que supera a limitada conceituação de internet como um ambiente acessível apenas por computadores. Nessa toada, a norma utiliza-se da ideia de "terminal" e demonstra que qualquer dispositivo deve necessariamente ser considerado como potencial para as condutas praticadas por meio virtual.

Ou seja, observar-se então que é admissível a recepção da Carta do Conselho de Direito Humanos da ONU, a qual anseia:

> The promotion, protection and enjoyment of human rights on the Internet: *The Human Rights Council*, *Guided* by the Charter of the United Nations, *Reaffirming* the human rights and fundamental freedoms enshrined in the Universal Declaration of Human Rights and relevant international human rights treaties, including the International Covenant on Civil and Political

[30] Constituição Federal da Republica do Brasil
[31] SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. 2ed. – São Paulo: Saraiva, 2015, p.25.

Rights and the International Covenant on Economic, Social and Cultural Rights,[32]

Recalling all relevant resolutions of the Commission on Human Rights and the Human Rights Council on the right to freedom of opinion and expression, in particular Council resolution 12/16 of 2 October 2009, and also recalling General Assembly resolution 66/184 of 22 December 2011,[33]

Noting that the exercise of human rights, in particular the right to freedom of expression, on the Internet is an issue of increasing interest and importance as the rapid pace of technological development enables individuals all over the world to use new information and communications technologies,[34]

Taking note of the reports of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, submitted to the Human Rights Council at its seventeenth session,[35] and to the General Assembly at its sixty-sixth session,[36] on freedom of expression on the Internet,[37]

1. *Affirms* that the same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice, in accordance with articles 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights;[38]

2. *Recognizes* the global and open nature of the Internet as a driving force in accelerating progress towards development in its various forms;[39]

3. *Calls upon* all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries;[40]

4. *Encourages* special procedures to take these issues into account within their existing mandates, as applicable;[41]

---

[32] Tradução: *O Conselho dos Direitos Humanos*,
Guiado pela Carta das Nações Unidas,
Reafirmando os direitos humanos e liberdade fundamentais consagradas na Declaração Universal dos Direitos Humanos e tratados universais de direitos humanos pertinentes, incluindo o Tratado Internacional sobre Direitos Civis e Políticos, e o Tratado Internacional sobre Direitos Econômicos, Sociais e Culturais,

[33] Tradução: Recordando todas as resoluções relevantes da Comissão de Direitos Humanos e Conselho de
Direitos Humanos sobre o direito de liberdade de opinião e expressão, em particular na resolução 12/16 de 2 de Outubro de 2009 do Conselho, e ainda recordando a resolução 66/184 de 22 de Dezembro de 2001 da Assembleia Geral,

[34] Notando que o exercício de direitos humanos, em particular o direito de liberdade de expressão, na Internet é um problema de crescente interesse e importância quanto o ritmo acelerado de desenvolvimento tecnológico que permite indivíduos de todos os lugares do mundo a usarem novas informações e tecnologias comunicadoras,

[35] A/HRC/17/27.

[36] A/66/290.

[37] Tradução: Tomando nota para os relatórios do Relator Especial sobre a promoção e proteção do direito de
liberdade de opinião e expressão, submetido no Conselho dos Direitos Humanos em sua décima sétima sessão,¹ e para a Assembleia Geral em sua sexagésima sexta sessão,² sobre liberdade de expressão na Internet,

[38] 1. Afirma que os mesmos direitos que as pessoas tem off-line também devem ser protegidos online, em particular a liberdade de expressão, que é aplicada independentemente de fronteiras e através de qualquer meio de escolha do indivíduo, de acordo com o artigo 19 da Declaração Internacional dos Direitos Humanos e Conselho Internacional dos Direitos Civis e Políticos;

[39] 2.Reconhece a natureza global e aberta da Internet como uma força motriz para acelerar o progresso rumo ao desenvolvimento em suas diversas formas;

[40] 3.Apela a todos os Estados para promover e facilitar o acesso a Internet e para cooperação internacional no desenvolvimento de mídia e informação e de facilidades de comunicação em todos os países;

[41] 4.Incentiva procedimentos especiais para tomar em conta estas questões dentro de seus mandatos

> 5. *Decides* to continue its consideration of the promotion, protection and enjoyment of human rights, including the right to freedom of expression, on the Internet and in other technologies, as well as of how the Internet can be an important tool for development and for exercising human rights, in accordance with its programme of work."[42]

Nesse interim, somando a definição de Direito Fundamental para o mestre José Afonso da Silva,[43] "que consiste em uma limitação imposta pela soberania popular aos poderes constituídos do Estado que dele dependem, de modo a assegurar uma convivência digna, livre e igual à todas as pessoas," à ideia da Internet, a qual abriga os direitos fundamentais de quarta geração, produto da globalização política na esfera da normatividade jurídica, que corresponde a sua institucionalização em nível internacional, como o direito à democracia e o direito à informação, a liberdade de expressão (emitir e receber uma informação); temos que ela é uma solução avançada para as comunicações já que supre uma série de problemas de inclusão, sendo portanto uma mídia democrática, que inclusive viabiliza o acesso da população as informações produzidas pelos órgão públicos.

Com isso cumpre notar que a Rede não é uma mera ferramenta, ou mais uma tecnologia, senão, um meio de comunicação o qual impacta na efetivação dos Direitos Fundamentais. Ao lado disso Ivar Alberto Martins Hartmann discorre que:

> há uma necessidade histórica do povo brasileiro de acesso à Rede, que, associada aos requisitos para a caracterização de um direito materialmente fundamental, permite a constatação de que o acesso à Internet é um Direito Fundamental pela Constituição de 1988. O direito é relevante para os indivíduos, na medida em que diversos aspectos da vida social vêm a ele ligar-se, requisitando o livre acesso de todos à rede mundial de computadores. O conteúdo do direito é a manutenção, pelo Estado, de terminais de acesso em condições de operação. O direito decorre dos princípios fundamentais da cidadania, pois relacionado com a fiscalização da atuação Estatal, bem como a participação popular no governo, e da dignidade, pois elementar à noção de autonomia, identidade pessoal e acesso à informação.

É manifesta a necessidade de um evolução legal para adaptar-se a essa esfera informatizada, a fim de que o Direito Penal e o Civil possam assegurar os direitos on-line e off-line de cada cidadão e que esses tenham então condições de

---

existentes, conforme o caso;

[42] 5.Decide continuar essa consideração de promoção, proteção e satisfação dos direitos humanos, incluindo o direito de liberdade de expressão, na Internet e em outras tecnologias, bem como toda Internet pode ser uma importante ferramenta para o desenvolvimento e para o exercício dos direitos humanos, de acordo com o seu programa de trabalho.

[43] SILVA, José Afonso da. Curso de direito constitucional positivo. 20. ed. São Paulo: Malheiros, 2001, p. 178.

exercer sua autonomia, identidade pessoa e sobretudo o acesso à informação e comunicação.

Outrossim, não é porque essa proteção e necessária e também é possível monitorar as atividades do indivíduo comum, dos infinitos bancos de dados, que o governo poderá exceder seus poderem de modo a suprimir a liberdade deste, ou constituir empecilhos para o progresso. Como sustenta Perez Luño[44], deverá haver apenas um pequeno "cuidado com a excelência e a popularização da rede porquanto ocorre a abertura de portas para malefícios que podem assolar a sociedade".

Malefícios como a violação da intimidade, privacidade, discursos discriminatórios ou de apologia ao terrorismo. Afinal a Internet embora pareça uma dimensão diferente da qual o homem vive, na verdade é apenas uma extensão desta. E todas as suas ações executadas nessa esfera são as mesmas que a do mundo físico, apenas se intensificam ou possuem maior facilidade de execução pois há ao mesmo tempo um acesso a número maior de vítimas propensas a estes delitos como também a propagação destes é mais extensa.

Esse temor justificado se dá ao poder de difusão de qualquer pensamento, qualquer ideia na internet. Uma vez que manche a reputação de uma empresa, cometa um crime de injúria, difamação não haverá um remédio, uma forma de desfazer o mal causado.

[44] PÉREZ LUÑO, A.E. **Derechos Humanos, Estado de Derecho y Constitución**, Tecnos, Madrid, 2.a ed. 1986, p.399

3. DOS CRIMES CIBERNÉTICOS

3.1 CONCEITO

Há divergência na doutrina acerca da denominação dada aos delitos cometidos por meio de um computador ou tecnologia similar, como o elucidado no artigo 154-A do Código Penal. Em princípio a mais proclamada é a cibercrimes; frise-se que esta não esta totalmente inadequada, ou correta, todavia é necessário lembrar que a Internet, assim como as tecnologias que a antecederam está em constante desenvolvimento, e não é aconselhável restringir a atuação do Direito aos crimes praticados tão somente por via dela, desta maneira a mais abrangente seria cibercrimes, e junto a ela a de crimes informáticos, em razão do bem jurídico tutelado.

Higor Vinicius Nogueira Jorge e Emerson Wendt[45] sustentam que "os crimes cibernéticos são aqueles que podem ou não ser praticados pelo meio informático." Nesta linha, o especialista na investigação de cibercrimes, Leonardo Andrade[46] entende que:

> Os cybercrimes nada mais são do que infrações penais cometidas no ciberespaço ou por meio dele, utilizando-se de recursos tecnológicos para sua consecução. Sendo esta a mais apropriada, pois se coaduna com o modelo da política criminal internacional instituída pela Convenção de Budapeste sobre Cybercrimes, modelo este, amplamente adotado por vários países.

Spencer Toth Sydow[47] possui opinião diversa desta, para ele há uma segunda denominação conveniente, a qual é difundida em razão do artigo 154-A, sobre crimes informáticos.

> A expressão crimes informáticos não e adotada de maneira uniforme pela doutrina, que apresenta outras nomenclaturas para o mesmo estudo, quais sejam, exemplificativamente, "crimes da era da informação", "crimes mediante computadores", "crimes cibernéticos", "cibercrimes", "crimes de computador", "crimes eletrônicos", "crimes tecnológicos", "crimes digitais", "crimes high-tech", "tecnocrimes", "netcrimes", "crimes virtuais", "crimes da tecnologia da informação" e até mesmo "e-crimes. Nossa opção pelo termo

---

[45] WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012.

[46] https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais

[47] SYDOW, Spencer Toth. **Crimes Informáticos e suas vítimas**. 2ed. – São Paulo: Saraiva, 2015, p.55-56.

> se dá com base no intuito amplo de tratar de uma criminalidade que não esta limitada às tecnologias existentes nem limitadas à Internet ou aos computadores, mas sim àquelas condutas que vão utilizando um novo ferramental conforme evolui o ser humano e a ciência – seja a nanotecnologia, a telefonia, a computação, a robótica ou qualquer outro ramo que crie aparatos facilitadores das tarefas diuturnas.

Consoante a isso, Túlio Vianna e Felipe Machado[48] afirmam que a denominação dada para um delito advém do nome do bem jurídico que deve ser salvaguardado; deste modo o crime de acesso não autorizado a dispositivo informático busca a proteção dos dados armazenados na ferramenta, e a ciência que a estuda é a Informática, portanto a correta definição recai como sendo "crimes informáticos" ou delitos "informáticos".

> Assim, esta claro que a denominação mais precisa para os delitos ora em estudo é " crimes informáticos" ou "delitos informáticos", por se basear no bem jurídico penalmente tutelado que é a inviolabilidade das informações automatizadas (dados).

Pensamento semelhante a Rita de Cássia[49], que adota a terminologia reconhecida pela Organização para a Cooperação Econômica e Desenvolvimento (OECD):

> Diante disso, a nominação *crimes informáticos*[50] parece ser a mais adequada por se tratar de expressão que se refere não soa o equipamento eletrônico em si, mas também a toda a tecnologia que possa ser por ele utilizada. Abrange, ainda, condutas que possam estar ligadas à informação e à sua transmissão isolada ou em conjunto.

Outro conceito a ser analisado neste trabalho é o de crimes virtuais. É aquele cometido por meio de um computador e conectado a Rede, como descreve o jurista Emanuel Gimenes[51].

> Em outras palavras, o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores (Internet) seja o instrumento ou o objeto do delito.

---

[48] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos.** Belo Horizonte: Fórum, 2013, p.21.
[49] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático.** São Paulo: Editora Revista dos Tribunais, 2003.
[50] Refere-se a uma modalidade de crime, especificamente, em que se vê a informática como elemento classificador; abrange todos os crimes em que se verifique o elemento sistema informático em sua composição.
[51] http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html

A fim de dar continuidade, nesse trabalho adota-se o termo crimes cibernéticos igual à definição de Wendt e Nogueira[52]:

> (...) decidimos utilizar o termo “crimes cibernéticos” para define os delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral). (...) Essas condutas indevidas praticadas por computador” podem ser divididas em “crimes cibernéticos” e “ações prejudiciais atípicas”. A espécie “crimes cibernéticos” subdivide-se em “crimes cibernéticos aberto” e “crimes cibernéticos exclusivamente cibernéticos”.

Referindo-se as “ações prejudiciais atípicas” são aqueles procedimentos, perpetrados por meio da rede mundial de computadores, que determinam alguma desordem e/ou dano para a vítima, entretanto não tem uma previsão penal, ou seja: o indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade.

3.2 HISTÓRICO

Da mesma forma que a Internet é extremamente recente, os crimes cibernéticos aparentam ser também, embora isso não seja verdade, realmente até a pouco não possuíam destaque para punições específicas, sendo necessário valer-se de um resultado, um dano, ou especial fim de agir de condutas já conhecidas pelo Direito Penal para adequá-lo, como expõe Victor Gonçalves[53]:

> Até a aprovação da Lei n. 12.737/2012, a punição por crimes cibernéticos somente era possível na forma da legislação comum, na medida em que não havia crimes específicos em relação ao tema. Para que referida punição fosse possível, entretanto, mostrava-se necessário algum resultado posterior (a subtração de valores, o dano, a ofensa à honra etc.).

Apenas em 2012, graças a interesses políticos e repercussão midiática é que foi aprovada a Lei 12.737, a qual alterou o Código Penal e então houve a criminalização de um comportamento específico. Junto a ele o Projeto da Lei Azeredo, que tramitava desde 1999, alterado inúmeras vezes, também foi sancionado pela Presidente; este tipificou as condutas realizadas mediante uso de

---

[52] WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012, p. 18.

[53] Victor Eduardo Rios Gonçalves. “**Direito penal esquematizado®**: parte especial - 6ed.” iBooks.

sistema eletrônico, digital ou similar, que fossem praticadas contra sistemas informatizados e análogo.

E dois anos mais tarde, foi instituído o Marco Civil da Internet no Brasil, que discute tão somente a liberdade de expressão, a neutralidade da Rede, o direito a privacidade, bem como os deveres e responsabilidades da guarda, proteção e publicação dos conteúdos deste meio. Quando também era esperado um conteúdo mais denso, abrangente e que proporcionasse um sentimento maior de segurança aos usuários e sobretudo aos cidadãos.

Estas modificações foram de extrema valia, úteis, mas ressalva-se no entanto que o objetivo maior não é possível com a simples aprovação de leis mal-acabadas e de aplicabilidade duvidosa como o Projeto de Lei 7.758/14, no qual discute o uso de perfil falso nas redes sociais.

a) Lei 12.737/2012

Lei advinda do Projeto de Lei 2.793/2011, aprovada por interesses políticos e pressão midiática em decorrência do vazamento de imagens e posterior tentativa de extorsão à atriz Carolina Dieckman, que "dá o nome" a Lei.

Esta lei com quatro artigos, tipifica fatos cibernéticos e altera os artigos 154, 266 e 298 do Código penal ao criar o delito de invasão de dispositivo informático, aumentou a pena para a invasão com prejuízo econômico, qualificou a obtenção de conteúdo sigiloso e a invasão por controle remoto e acrescentou o delito de interrupção de serviço informático.

Infelizmente segundo Damásio de Jesus[54] ela "não trata da estrutura investigativa ou deveres dos provedores de Internet e serviços no que tange à cooperação para com autoridades na investigação de crimes digitais".

> Em seu primeiro artigo, informa que disporá sobre a tipificação penal de delitos informáticos, no plural. Porém, o que se vê, na sequência (art. 2°), e que somente houve criação legislativa de um delito de tal natureza, denominado "invasão de dispositivo informático."
> No terceiro artigo, o que se fez foi alargar a incidência do tipo penal do art. 266, bem como o do art. 298, ambos do Código Penal, sem inovação legislativa propriamente dita, mas sim abarcando situações que antes não poderiam gerar consequências penais pela inexistência específica de precisão (logicamente, portanto, limitado pelo princípio da legalidade) e pela proibição da interpretação analógica *in malan partem* e ausência de

[54] JESUS, Damásio de. **Manual de crimes informático**. São Paulo: Saraiva, 2016, p. 152.

> permissão para extensão da interpretação no texto legal (SYDOW; 2015, p.288)

b) Lei 12.735/2012

Originário do Projeto de Lei 84/99, o qual derivava do PL n. 1.713/96. Mesmo após significativos debates e consulta pública, devido à influências políticas e da Convenção de Budapeste sofreu vários apensamentos e modificações de forma a fugir completamente de seu objetivo de com 18 artigos modificar o Código Penal a fim de definir e criminalizar condutas relacionadas a informática.

Sua efetividade é questionada pois foram pequenos os impactos na área jurídica, como fomenta Spencer Toth Sydow[55]:

> O projeto inicial – que buscava apresentar princípios, dar definições e criminalizar condutas de dano informático, acesso indevido, alterações de dados, obtenção indevida de dados, violação de segredo e produção de *malwares* em 18 artigos que alterariam o Código Penal – foi aprovado apenas 6, sendo que apenas um deles modificou o Código Penal, um alterou o Código Penal Militar e um alterou a Lei n. 7.716/89 (lei que define os crimes resultantes de preconceito de raça ou de cor).
> (...)
> Perdeu-se a maior parte dos tipos penais inovadores para se conseguir a aprovação de algum normativo na área de crimes informáticos, desperdiçando-se muitos anos de trabalho.

c) O Marco Civil da Internet (Lei 12.965/2014)

Para Iso Chaitz Scherkerkewitz[56] o Marco Civil da Internet é a Constituição deste meio:

> é a “Constituição” da Internet, ou seja, é a Lei que traça as diretrizes, as normas fundamentais da Rede no Estado Brasileiro”.
> (...)
> “ A existência de um Marco Civil para a Internet é uma tomada de posição do Estado brasileiro que entende a Rede não como um simples avanço tecnológico, que possibilita inegáveis fatores de progresso econômico, mas, sim, como algo que pode fortalecer a cidadania e aumentar a cultura do povo.
> (...)
> Em muitos quesitos da lei o Brasil foi pioneiro, mesmo porque, no mundo inteiro ainda se discute a necessidade do controle da Internet e o papel do Estado nesse controle, sendo assim, somos precursores no tocante à governança da Internet.

[55] SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. 2ed. – São Paulo: Saraiva, 2015, p.279-280.
[56] SCHERKERKEWITZ, Iso Chaitz. Direito e Internet. São Paulo: Editora Revista dos Tribunais, 2014, p.47-48.

Entretanto o Marco Civil não é a Constituição da Internet, primeiro por trata-se de uma lei muito específica e portanto incapaz de cumprir um papel tão importante, e inclusive falhar ao não contemplar um número significativo de pontos para assim reger e proteger a todos; segundo porque não diz respeito ao controle do indivíduo na Rede, uma vez que seu foco é a responsabilidade dos provedores frente a fragilidade dos usuários, junto à neutralidade da Rede e do acesso as informações, assunto que tem muito a ser discutido (veja o exemplo do bloquei o do Whats App).

Para Spencer Toth Sydom[57] esta Lei busca na verdade a "criação de margens seguras para deveres e responsabilidades – no caso concreto aos usuários e aos prestadores de serviço na internet." Apesar de sucinta e lacunosa é capaz de influenciar diretamente na construção e aplicação do Direito Penal.

> A criação expressa de valores como inviolabilidade do usuário, de suas comunicações e seus dados apresenta uma nova realidade merecedora de proteção. E o direito penal necessita de valores legitimados para que bens jurídicos protegidos possam surgir legitimamente.

Adiante, Iso Chaitz Scherkerkewitz[58] dispõe que é imperativo compreender que o Estado não possui um poder de censura, nem deve exerce-lo a tal ponto a fim de respeitar o Princípio da Intervenção Penal Mínima; o que se espera é um mínimo de regras para assegurar a proteção da liberdade de expressão e os demais direitos que o indivíduo possui e não é porque faz uso da Internet deverão ser preteridos.

> Entendemos que, que a ideia de que o Estado não deve se envolver nos assuntos relacionados à Rede, ficou de há muito superada, em virtude do potencial de danos que podem ser provocados ao cidadão, se não houver um mínimo de regras que estipulem os direitos e responsabilidades dos usuários.
> Não se defende a existência de regras de censura, mas sim, a existência de regras de responsabilidade(direito civil x penal), que deverão ser obedecidas pelos operadores do sistema, visando a preservação da liberdade de expressão, do acesso ao próprio sistema e do direito a intimidade e a privacidade.

d) Convenção de Budapeste

[57] SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. 2ed. – São Paulo: Saraiva, 2015, p. 275.
[58] SCHERKERKEWITZ, Iso Chaitz. Direito e Internet. São Paulo: Editora Revista dos Tribunais, 2014, p. 49.

Trata-se de um tratado internacional de direito penal e processual penal sobre cibercrimes, criada na Hungria em 23.11.2001, pelo Conselho da Europa, na qual 20 países tipificam e buscam a adoção de medidas contra a criminalidade exercida no ciberespaço. Mais precisamente um Regime Internacional de auxilio mútuo, isto é, que fomente a cooperação entre estes membros e ainda, entre Estados e a Indústria para tornar este combate mais eficaz.

> The member States of the Council of Europe and the other States signatory hereto, *Considering that* the aim of the Council of Europe is to achieve a greater unity between its members;[59]
> *Recognising the* value of fostering co-operation with the other States parties to this Convention;[60]
> *Convinced of* the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation;[61]
> *Conscious of* the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;[62]
> *Concerned by* the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;[63]
> *Recognising the* need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;[64]
> *Believing that* an effective fight against cybercrime requires increased, rapid and well functioning international co-operation in criminal matters; [65]
> *Convinced that* the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;[66]

---

[59] Tradução: Os Estados membros do Conselho da Europa e os seguintes Estados signatários, Considerando que o objetivo do Conselho da Europa é realizar uma união mais estreita entre os seus membros;

[60] Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes da presente Convenção;

[61] Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;

[62] Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;

[63] Tradução: Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;

[64] Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;

[65] Acreditando que uma luta efetiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;

[66] Convictos de que a presente Convenção é necessária para impedir os atos praticados contra a

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;[67]
Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal;[68]
Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;[69]
Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;[70]
Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;[71]
Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of

---

confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adoção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável;

[67] Tendo presente a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano, tal como garantidos pela Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, pelo Pacto Internacional sobre os Direitos Civis e Políticos das Nações Unidas de 1966, bem como por outros tratados internacionais aplicáveis em matéria de direitos do Homem, que reafirmam o direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras e, ainda, o direito ao respeito pela vida privada;

[68] Tendo igualmente presente o direito à proteção de dados pessoais, tal como é conferido, por exemplo, pela Convenção do Conselho da Europa de 1981, para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal;

[69] Tradução: Considerando a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, e a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil de 1999;

[70] Tendo em conta as convenções existentes do Conselho da Europa sobre a cooperação em matéria penal, bem como outros tratados similares celebrados entre os Estados membros do Conselho da Europa e outros Estados, e sublinhando que a presente Convenção tem por finalidade complementar as referidas convenções, de modo a tornar mais eficazes as investigações e as ações penais relativas a infracções penais relacionadas com sistemas e dados informáticos, bem como permitir a recolha de provas em forma electrónica de uma infracção penal;

[71] Saudando os recentes desenvolvimentos destinados a aprofundar o entendimento e cooperação internacionais no combate à criminalidade no ciberespaço, nomeadamente, as ações empreendidas pelas Nações Unidas, pela OCDE, pela União Europeia e pelo G8;

> copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;[72]
> *Having regard* to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;[73]
> *Having also* regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;[74]

Apesar do Brasil não ser um dos estados membros, ele como convidado poderia à aderir a Convenção, e durante a discussão do Projeto de Lei Azeredo, que deu origem a Lei 12.735/2012, levantou-se tal ponto mas até o momento priorizou a criação de suas próprias leis e não se posicionou sobre a adesão apesar de ter bom relacionamento com os países em questão.

---

[72] Recordando as Recomendações do Comité de Ministros N.º R (85) 10 relativa à aplicação prática da Convenção Europeia sobre Auxílio Judiciário Mútuo em Matéria Penal quanto às cartas rogatórias para a intercepção de telecomunicações, N.º R (88) 2 sobre as medidas destinadas a combater a pirataria no domínio do direito de autor e dos direitos conexos, N.º R (87) 15 que regula a utilização de dados de carácter pessoal no sector da polícia, N.º R (95) 4 relativa à proteção dos dados de carácter pessoal no sector das telecomunicações, tendo em conta, designadamente os serviços telefónicos e a N.º R (89) 9 sobre a criminalidade informática que estabelece diretrizes para os legisladores nacionais respeitantes à definição de certos crimes informáticos e, ainda, a N.º R (95) 13 relativa a problemas processuais penais relacionados com as tecnologias da informação;

[73] Tradução: Tendo em conta a Resolução n.º 1 adoptada pelos Ministros Europeus da Justiça na sua 21ª Conferência (Praga, 10 e 11 de Junho de 1997), que recomenda ao Comité de Ministros para apoiar o trabalho desenvolvido pelo Comité Europeu para os Problemas Criminais (CDPC) sobre a cibercriminalidade a fim de aproximar as legislações penais nacionais e de permitir a utilização de meios de investigação eficazes em matéria de crimes informáticos, bem como a Resolução n.º 3, adoptada na 23ª Conferência dos Ministros Europeus da Justiça (Londres, 8 e 9 de Junho de 2000), que incentiva as partes intervenientes nas negociações a prosseguirem os seus esforços para encontrar soluções apropriadas que permitam o maior número N possível de Estados a tornarem-se Partes da Convenção e reconhece a necessidade de dispor de um mecanismo rápido e eficaz de cooperação internacional, que tenha devidamente em conta as exigências específicas da luta contra a cibercriminalidade;

[74] Tendo igualmente em conta o Plano de Ação adoptado pelos Chefes de Estado e de Governo do Conselho da Europa, por ocasião da sua Segunda Cimeira (Estrasburgo, 10 e 11 de Outubro de 1997), para procurar respostas comuns face ao desenvolvimento das novas tecnologias da informação, com base nas normas e princípios do Conselho da Europa;

3.3 TIPIFICAÇÃO PENAL

Para Túlio Vianna e Felipe Machado[75] não é qualquer conduta que caracterizará um delito informático, mas somente a que assinalar-se merece a atenção do Direito Penal:

> O Direito Penal não se ocupa de qualquer conduta humana, pois somente aquelas que constituem infrações penais são para ele relevantes. Assim, a conduta de invadir dispositivo informático será objeto valido de estudo para o Direito e Processo Penal caso constitua uma infração penal.

O meio utilizado pelos hackers e crackers não contempla apenas o computador e a internet. Com a sofisticação dos aparelhos eletrônicos e meios de comunicações e a agilidade com que estes chegam ao mercado, atraem grandes massas, ainda que com preços exorbitantes, é possível dizer que praticamente qualquer objeto com uma luz de LED ou capaz de gerar ondas é alvo ou pode ser capaz de servir de meio para a prática de delitos ou ainda ser fonte da curiosidade aguçada destes indivíduos.

Um exemplo são os consoles de vídeo games que além da função original, passaram a armazenar informações, replicam o sinal de Wi-fi e ganharam grande apreço por curiosos e criminosos que passaram a servir-se desta ferramenta para tentar cometer delitos sem que sejam deixados rastros.

O mesmo vale para o modem de Wi-fi, o qual possui codificação simplificada, e muitas vezes suas redes não são seguras. Assim facilmente qualquer indivíduo pode invalidá-la cometer fraudes sem deixar os rastros e ainda incriminar o proprietário, uma vez que este é o responsável pelas ações praticadas nela; especialmente porque no Brasil ainda não há tantos recurso, e tampouco é comum e realizar o caminho contrário do delito para tentar identificar o IP da máquina empregada para tal ação.

A diferença de tratamento e a importância dada a esta ferramenta é que na Alemanha, sequer os grandes aeroportos possuem redes livres, como Wi-fi gratuitos; há a exigência de um cadastro prévio e um alto custo por hora, isso tudo como mecanismo de tentar eximir seus proprietários de serem responsabilizados por atos praticados por usuários mal intencionados.

---

[75] VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013, p. 15.

A atuação do hacker se dá por acessos. Qualquer ação do homem com o computador, que modifique, leia, ou processe dados, como expõe Túlio Vianna e Felipe Machado[76]:

> Acesso é a ação humana de ler, escrever ou processar dados armazenados em sistemas computacionais.
> Ler dados armazenados em um dispositivo informático consiste em reinterpreta-los como informações humanamente inteligíveis. A leitura de um texto, a visualização de fotos e a audição de musicas armazenadas em computador são exemplos de leitura de dados.
> (...)
> "Caso leia uma informação exibida em um monitor, recupera-se dados; caso se clique com o mouse em algum ponto da rela ou se pressione a barra de espaço do teclado, inserem-se dados; caso se altere o nome de um arquivo, modificam-se dados; caso se desligue o computador, apagam-se dados da memoria RAM. (grifo nosso)

Para o mesmo autor[77] esses acessos são classificados em permissões, forma pela qual legitima-se e é possível o ingresso de cada usuário aos arquivos e diretórios de um sistema, seja para acrescentar, modificar ou apagar o seu conteúdo. Ou seja, se dá por meio da leitura, escrita ou execução.

> O usuário que criou o arquivo no dispositivo informático, em princípio reta plenos poderes em relação ao respectivo item, podendo lê-lo, alterá-lo e, caso seja um programa ou um script, executa-lo. Aos demais, na maioria das vezes, é permitida somente a leitura do arquivo, quando muito.

Assim, de modo geral, todo indivíduo terá alguma autorização, de níveis distintos, ao que está armazenado tanto no computados como na Rede; enquanto que os hackers costumeiramente transpõe estas autorizações, como cita Túlio Vianna e Felipe Machado[78]:

> A autorização e a legitimação jurídica que alguém possui para acessar determinados conteúdos dados e um dispositivo informático. Sua validade decorre da propriedade dos dados, sendo que o proprietário dos dados, evidentemente, terá sempre plenos poderes para acessá-los. Poderá ele também permitir que outras pessoas tenham acesso a esses dados, autorizando-as, geralmente, através da concessão de uma senha. Presume-se que aquele que tenha a permissão para acessar um arquivo também tenha autorização do proprietário para fazê-lo. Ocorre, no entanto, que, em determinados casos , a pessoa tem o poder de acessar os dados – permissão de acesso – porém não tem a autorização jurídica do proprietário para faze-lo. E o que ocorre nos casos de excesso no acesso autorizado a dispositivos informáticos.

[76] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013, p.26.
[77] ibid, p. 27.
[78] Ibid, p. 27-28.

Além de tratar do meio em que os hackers e crackers atuam, e da forma como se dá o acesso, é necessária a compreensão de que este pode ocorrer tanto por via remota, ou seja online, como local, off-line, igual descreve Vianna e Machado[79]:

> O acesso local é aquele em que o agente tem o contato físico com o dispositivo informático que acessa, emitindo seus comandos através de um dispositivo de entrada de dados (teclado, mouse, etc.) diretamente conectado ao dispositivo acessado. Pode se dar às escondidas, ou mesmo, mediante violenta ou grave ameaça à pessoa. (...) O acesso remoto é o método mais comum de invasão de dispositivos informáticos. Não há qualquer contato físico do cracker com o dispositivo invadido, além de que o computador utilizado pelo agente para emitir os comandos de acesso é diferente daquele em que os dados estão armazenados. A invasão se dá através de uma rede que, na maioria absoluta das vezes, é a Internet.

Fica claro que assim como todo hacker não é necessariamente um ckacker, nem todo usuário com acesso autorizado, é de fato o proprietário ou dotado de toda a autorização necessário para ler, modificar ou executar um conteúdo. E isso pode ocorrer com ou sem o auxílio da Internet. Daí decorre a necessidade de rever a responsabilidade e punibilidade de quem o faz.

3.4 ASPECTOS DOGMÁTICOS

Os crimes cibernéticos possuem um padrão, uma característica que os torna *sui generis*, que é a violação a particularidade individual, a privacidade acerca dos dados e informações contidos em um dispositivo informático como cita Spence Toth Sydow[80]:

> Os Delitos informáticos exigem algumas regras-padrão a partir das quais todo o raciocínio jurídico-penal se monta e das quais emanam características que se aplicam a todo um cabedal de condutas. São elementos dos quais nascem os fenômenos atinentes à violação da segurança informática ou à nova ferramenta para lesionar de maneira inovadora os basilares bens jurídicos.

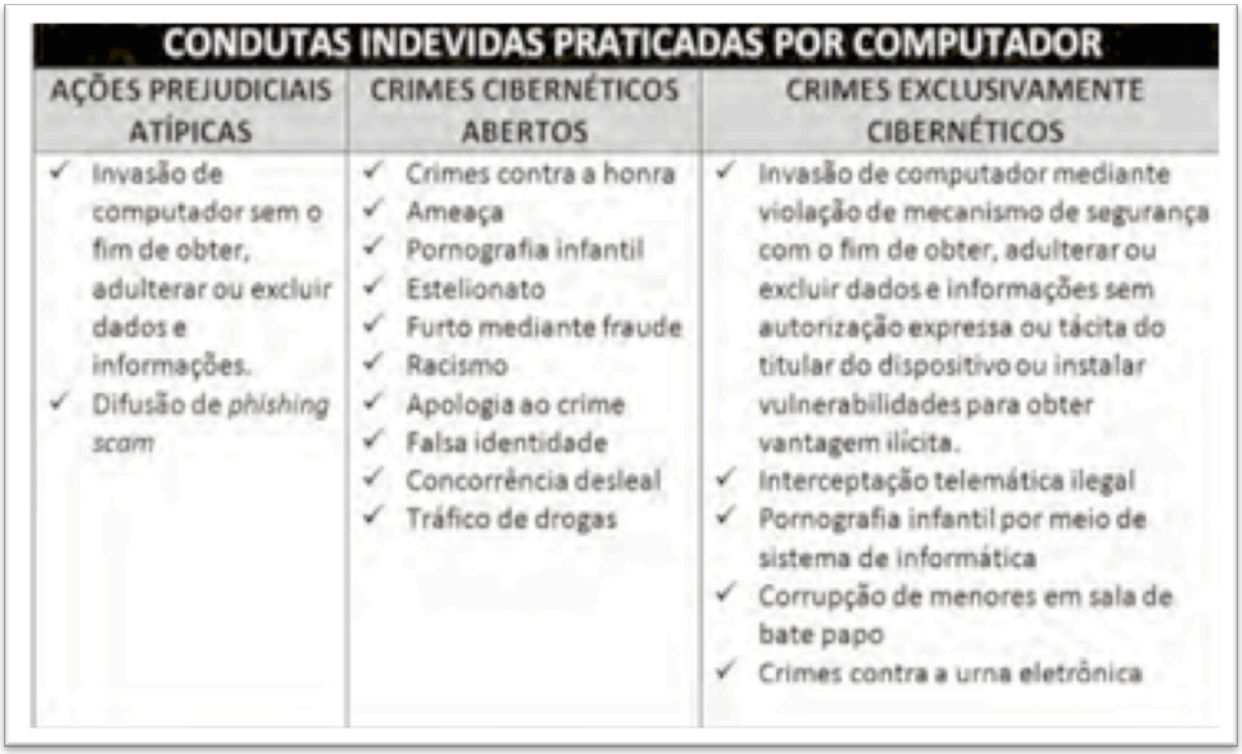
Desta forma, existe uma diferença entre crime cometidos por intermédio da informática e os cibercrimes; os do primeiro tipo são por exemplo os crimes de pornografia infantil, pirataria de software, ameaça, injúria, todos abarcados devidamente pelo código penal; diferente dos crimes do segundo tipo, que merecem ser analisados, e pode variar conforme a legislação de um país para o outro. Como

[79] VIANNA, Túlio; MACHADO, Felipe. Crimes informáticos. Belo Horizonte: Fórum, 2013, p. 65.
[80] SYDOW, Spencer Toth. Crimes Informáticos e suas vítimas. 2ed. – São Paulo: Saraiva, 2015, p.89.

específica o juiz federal Emanuel Gimenes:

> Em outras palavras, o crime virtual é qualquer ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão em que um computador conectado à rede mundial de computadores (Internet) seja o instrumento ou o objeto do delito.

Wendt e Nogueira[81] seguem este pensamento e o específica ainda mais ao classificar os delitos informáticos como sendo crimes cibernéticos exclusivos e crimes cibernéticos abertos, conforme pode ser visto na tabela a seguir:



CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR

AÇÕES PREJUDICIAIS ATÍPICAS	CRIMES CIBERNÉTICOS ABERTOS	CRIMES EXCLUSIVAMENTE CIBERNÉTICOS
✓ Invasão de computador sem o fim de obter, adulterar ou excluir dados e informações. ✓ Difusão de *phishing scam*	✓ Crimes contra a honra ✓ Ameaça ✓ Pornografia infantil ✓ Estelionato ✓ Furto mediante fraude ✓ Racismo ✓ Apologia ao crime ✓ Falsa identidade ✓ Concorrência desleal ✓ Tráfico de drogas	✓ Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. ✓ Interceptação telemática ilegal ✓ Pornografia infantil por meio de sistema de informática ✓ Corrupção de menores em sala de bate papo ✓ Crimes contra a urna eletrônica

Fonte: Wendt e Nogueira, 2012.

Os crimes cibernéticos aberto podem ser praticados na sua forma convencional, física ou por meio de um dispositivo informático, enquanto que os exclusivamente cibernéticos só poderão ser realizados por meio de dispositivo que possibilite o acesso à internet. Assim, Wendt e Nogueira[82] citando Coriolano Almeida Camargo entende que nos crimes exclusivamente cibernéticos geralmente o agente "utiliza da boa-fé da vítima e da sua distração para cometer o delito, no caso do roubo de dados bancários, algo diferente do estelionato, no qual o indivíduo

[81] WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012, p. 20.
[82] Ibid.

entrega suas informações".

Outra classificação existente, e muito similar, dada aos crimes informáticos é a adotada por Vianna e Machado,[83] e também aceita por Damásio de Jesus, a qual divide os delitos em próprios, impróprios, mistos e mediatos ou indiretos.

> Crimes informáticos impróprios são aqueles em que o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação (dados).
> (...) A Internet e os computadores são usados neste caso como instrumento para a pratica da conduta típica em sua modalidade de publicar. Aqui também se tem um crime informático improprio que em nada ofende o direito à inviolabilidade de dados, e portanto, deverá ser punido com o tipo penal já existente. (...) Dentre os crimes informáticos impróprios praticados na Internet destaca-se o crime de estelionato (art. 171, do CPB). As formas de execução deste delito as mais variadas e, em geral, seu sucesso depende da confiança que a vítima deposita nos autores.

Isto é, o crime informático improprio não tutela o bem jurídico do art. 154-A, a inviolabilidade dos dados. Já que nele o agente só se vale do computador ou da internet com meio para praticar um delito contra outro bem jurídico. Desta forma Damásio de Jesus[84], entende que nessa modalidade, "a legislação criminal é suficiente, pois grande parte das condutas realizadas já possui correspondência em algum dos tipos penais."

Diverso dos crimes informáticos próprios classificados pelos mesmos autores[85]:

> Crimes informáticos próprios são aqueles em que o bem jurídico protegido pela norma penal e a inviolabilidade das informações automatizadas (dados) (...) Já em relação à interceptação ilegal, esta é um crime informático próprio no qual os dados são capturados durante sua transferência de um dispositivo informático para outro. (...) Os delitos informáticos próprios, destaca-se, por fim, a criação e divulgação de programas de computadores destrutivos, que tem como principal representante os vírus informáticos. Esta conduta foi criminalizada, o que se deu o §1° do art. 154-A do CPB. (p.32-33)

Os crimes informáticos próprios tutelam a inviolabilidade dos dados informáticos. São aqueles praticados com a divulgação de vírus e programas destrutivos, ou é realizada a interceptação da troca de dados. Neste caso segundo

---

83 VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013, p. 30-31.
84 JESUS, Damásio; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 49.
85 ibid, p.32-33

Damásio de Jesus[86], “a legislação penal é lacunosa, em consequência do princípio da reserva legal, a qual faz com que muitas práticas não possam ser enquadradas criminalmente.”

O bem jurídico da inviolabilidade dos dados informáticos também será um dos tutelados pelos crimes informáticos mistos, como o exposto por Vianna e Machado:[87] “Crimes informáticos mistos são crimes complexos[88] em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa”.

Neste tipo há a confluências da proteção da inviolabilidade dos dados com outro bem jurídico distinto deste, originário de um outro tipo jurídico, devidamente resguardado pela legislação brasileira.

Resta ainda o crime informático indireto ou mediato que Vianna e Machado[89] descreve como “delito-meio não informático o qual herdou essa característica do delito-meio informático realizado para possibilitar sua consumação.” Complementarmente Damásio de Jesus[90] citando Marcelo Crespo, percebe que esta modalidade sequer deveria ser considerada como delito informático, pois tecnicamente não é o objeto do ilícito:

> Trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a pratica de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente será punido pelo delito-fim (furto). (...) “A simples utilização de um computador para a perpetração de um delito como um estelionato não deveria ser – repita-se – com precisão técnica, considerada um crime informático”. Ocorre, todavia, que não só autores, mas também a mídia em geral, convencionaram denominar crimes informáticos qualquer delito praticado com o uso da tecnologia, seja ela o instrumento da conduta, seja o objeto do ilícito.

Ora, nesta modalidade o delito informático só serviu de meio para a execução do delito principal e então ocorresse sua consumação.

Portanto é errônea a ideia de que qualquer delito empreendido por meio de um computador, com dispositivo informático ou que faz uso da Internet será reputado como crime cibernético próprio.

A partir destas noções torna-se possível analisar o artigo 154-A do Código

---

[86] JESUS, Damásio; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016, p. 48.

[87], ibid p. 34.

[88] Representa a união de mais de um tipo penal.

[89] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013, p. 35.

[90] JESUS, Damásio; MILAGRE, José Antônio. Op. cit. p. 48.

Penal.

4 DOS CRIMES DE ACESSO NÃO AUTORIZADO A SISTEMA INFORMÁTICO – ART.154-A

4.1 CONSIDERAÇÕES PRELIMINARES

A Lei n.º 12.737, de 30 de novembro de 2012 acrescentou ao Código Penal Brasileiro os artigos 154-A e 154-B:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1.º 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.
> § 2.º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3.º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constituir crime mais grave.
> § 4.º Na hipótese do § 3.º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5.º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

O presente artigo busca a defesa frente a crimes praticados contra a liberdade individual, contra a inviolabilidade dos segredos; protege-se assim a segurança telemática, mas peca ao deixar de abordar outras condutas violadoras neste referido tipo penal.

Como poderá ser visto a seguir este artigo possui redação confusa, lacunas e carecendo de revisão, ou adaptação.

4.2 BEM JURÍDICO PROTEGIDO

Segundo Luiz Regis Prado[91] o bem jurídico é "um ente (dado ou valor social) material ou imaterial haurido do contexto social, de titularidade ou metaindividual reputado como essencial à coexistência e desenvolvimento do homem" e, por isso, deve ser jurídico-penalmente protegido.

A par disso, o bem jurídico deste tipo penal pode ser dividido em dois: mediado e imediato. Assim, primeiramente há o enquadramento nos crimes contra a liberdade individual, e em um segundo plano se protege justamente a inviolabilidade dos dados informáticos, que segundo Guilherme Nucci[92]:

> A proteção se volta à intimidade, à vida privada, à honra, à inviolabilidade de comunicação e correspondência, enfim, à livre manifestação do pensamento, sem qualquer intromissão de terceiros. Sabe-se, por certo, constituir a comunicação telemática o atual meio mais difundido de transmissão de mensagens de toda ordem entre pessoas físicas e jurídicas. O e-mail tornou-se uma forma padrão de enviar informes e mensagens a profissionais e particulares, seja para fins comerciais, seja para outras finalidades das mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também o dispositivos informáticos, que mantém dados relevantes do seu proprietário. (grifo nosso).

Complementando tal posicionamento, Túlio Vianna e Felipe Machado[93] afirmam também que o bem jurídico tutelado é a inviolabilidade dos dados informáticos, originários do direto a privacidade e a intimidade e em concordância com o art. 5°, X da Constituição Federal; na qual: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;"

> O bem jurídico penalmente tutelado é a inviolabilidade dos dados informáticos, corolário do direito à privacidade e intimidade presentes na Constituição da Republica, em seu art. 5°, X. A inviolabilidade compreende não só o direito à privacidade e ao sigilo dos dados, como também à integridade destes e sua proteção contra qualquer destruição ou mesmo alteração.

---

[91] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro,** volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. – São Paulo: Revista dos Tribunais, 2013, p. 322.
[92] NUCCI, Guilherme de Souza. **Código Penal: Comentado.** 13. ed.. Rio de Janeiro - RJ: Forense, 2013, p. 744.
[93] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Forum, 2013. p. 94.

Nessa linha, o bem jurídico tutelado pelo artigo 154-A do Código Penal é a informação, a inviolabilidade dos dados informáticos e ainda a intimidade e a privacidade. Sendo o objeto material o dispositivo informático, estando ele conectado ou não a internet.

4.3 SUJEITO DO DELITO

a) Sujeito Passivo:

O sujeito passivo pode ser qualquer pessoa (física ou jurídica) proprietária de um dispositivo invadido ou que possuía dados e informações armazenadas nele. Para Victor Goncalves[94] "é a pessoa ou entidade que sofre os efeitos do delito (a vítima do crime) podendo em alguns crimes ser uma entidade sem personalidade jurídica, como a família, a sociedade etc."

Seguindo este pensamento, Túlio Vianna e Felipe Machado[95] advertem que neste delito o "sujeito passivo é qualquer pessoa, física ou jurídica, proprietária dos dados informáticos, ainda que não necessariamente do sistema computacional. Mesma ressalva apresentada por Rita de Cássia:[96]

> Os sujeitos passivos das ações aqui tratadas não guardam, para a sua identificação, nenhum cuidado especial. É o titular do bem jurídico lesado, ou ameaçado de lesão. Tanto poderá ser sujeito passivo a vítima ofendida, a pessoa física ou jurídica, o Estado, a coletividade, a comunidade internacional, dependendo, para a sua identificação, da natureza do delito.

b) Sujeito Ativo:

O sujeito ativo pode ser qualquer pessoa que cometa a conduta de invadir um dispositivo, até mesmo porque neste tipo penal não é exigida qualquer conduta especial. Victor Gonçalves,[97] apoia-se a isso e portanto "o sujeito ativo do crime é quem pode cometer determinada infração penal, quem executa a conduta típica descrita na lei e assim realiza o verbo contido no tipo penal." No caso do artigo 154-A é a pessoa que acessa os dados de um dispositivo informático sem que esteja

---

[94] GONÇALVES, Victor Eduardo Rios . **Direito penal esquematizado®** : parte especial – 6. ed. – São Paulo : Saraiva, 2016. – (Coleção esquematizado® / coordenação Pedro Lenza.) – p. 184.
[95] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Forum, 2013. p.95.
[96] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático**. São Paulo: Editora Revista dos Tribunais, 2003, p.82.
[97] GONÇALVES, Victor Eduardo Rios. op.cit. p. 179.

autorizada.

A partir disso, Túlio Vianna[98] define "o sujeito ativo como qualquer pessoa humana não autorizada a acessar os dados, exceto o proprietário do dispositivo informático no qual os dados estão armazenados".

Sobressai deste conceito um questionamento importante: Ainda que não autorizado o proprietário do dispositivo pode acessar os dados de quem a utilizou sem configurar crime? Sim. Para o referido autor estabelece assim uma "conduta atípica, absurda, pois o que se deve tutelar é a inviolabilidade dos dados, independente de quem seja o proprietário da máquina". Sendo assim, emerge a necessidade de correção desta lacuna pelo legislador, como afirma Vianna e Machado[99]:

> Ao optar pela expressão "invadir dispositivo informático alheio", o legislador tornou atípica as condutas de quem invade dispositivo informático próprio para obter indevidamente dados informáticos alheios lá armazenados. Em *lan houses* ou "*cyber cafés*", por exemplo, o proprietário dos dispositivos informáticos não praticara o crime se acessar sem autorização os dados do usuário que alugar a maquina. Da mesma forma, será atípica a conduta do empregador que acessar e-mails pessoais do empregado sem sua autorização armazenados em seu computador do trabalho.
> Trata-se obviamente de uma situação absurda, pois o que se deve tutelar é inviolabilidade dos dados, independentemente de quem seja o proprietário da maquina. Não há, porém, como interprete sanar o problema, pois a analogia *in malan partem* é vedada no Direito Penal pelo princípio da legalidade. Espera-se, pois, que o legislador corrija esta lacuna por meio de uma nova lei. (grifo nosso).

Nesta esteira, sujeito ativo será o que se conhece por Hacker. Numa definição corriqueira do dicionário Michaelis tem-se:

> *Hacker*
> *hac.ker*
> *(réker) (ingl) sm Inform.*
> *Pessoa viciada em computadores, com conhecimentos de informática, que utiliza esse conhecimento para o benefício de pessoas que usam o sistema, ou contra elas.*

Na concepção de Damásio de Jesus[100] não podemos definir todo hacker como alguém que irá produzir efeitos negativos ou não; apenas que é habilidoso com a informática. "Um Hacker é um profundo conhecedor de informática, podendo ser um profissional de segurança da informação ou pesquisador, que não utiliza

[98] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013. p.104
[99] Idem, p. 94-95.
[100] JESUS, Damásio; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016, p. 53.

seus conhecimentos para fins ilegítimos."

Sem embargo, segundo Rita de Cássia[101], tecnicamente, o termo advém do *Massachuts Institut of Technology* – MIT, onde Hackers eram os estudantes de computação, os especialistas em computador, que rompiam a noite realizando pesquisas. Frise-se que para a autora[102] a tradução mais adequada seria "fuçador" já que nem todos os hackers, que são indivíduos dotados de habilidades técnicas informáticas além do comum, ou ainda facilidade e disposição em manusear um computador de forma a aventurar-se nele, realmente as utilizam para cometer atos ilícitos. Esses devem ser denominados *hackers;* enquanto que o "invasor malicioso", também portador de grande conhecimento técnico mas com "potencial destrutivo, geralmente utilizado para adentrar servidores, o melhor meio para propagar informações e vale de sua experiência para a prática de crimes é na verdade o *ckacker"*.

Fica claro para Rita de Cássia Lopes da Silva[103], que nem sempre o cracker poderá ser considerado um criminoso em busca de vantagens econômicas:

> O que se observa é que os delinquentes da informática nem sempre vislumbram qualquer vantagem material com a conduta. Têm-se em mente o desafio ao equipamento, às regras de ética, pelo simples fato de poderem se satisfazerem e se vangloriar perante aos seus iguais, demonstrando, pelas ações e seus resultados, o que são capazes de realizar. Muitas vezes, o que move esse tipo de criminoso é o desafio, é o contato com o proibido. São por vezes verdadeiros anarquistas.

Por isso ficaram famosas situações em que estes indivíduos adentraram aos sistemas da Microsoft para ter acesso em primeira mão ao que fora criado, antes do lançamento, a Sony como boicote a suas novas políticas, a governos federais para tornar transparentes atos que até então foram omitidos e que deveriam ser de conhecimento dos cidadãos.

Por exemplo, no inicio de maio deste ano a Justiça Federal de Sergipe determinou o bloqueio do aplicativo WhatsApp em razão de da companhia dona do aplicativo ter se negado a fornecer as conversas de uma suposta quadrilha interestadual de trafico de drogas. Como represaria, por entenderem que o bloqueio fere a liberdade dos cidadãos e inclusive estaria prejudicando a comunicação de

---

[101] SILVA, Rita de Cássia Lopes da. **Direito Penal e Sistema Informático.** São Paulo: Editora Revista dos Tribunais, 2003, p.77.
[102] SILVA, Rita de Cássia Lopes da. Op. cit. p.78.
[103] Iíbid, p.80.

mais de 100 milhões de brasileiros o grupo Anonymos postou nas mídias sociais mensagens comprovando que havia derrubado diversos sites relacionados ao governo de Sergipe. Tem-se então uma conduta atípica, pois apesar de gerarem uma instabilidade momentânea nos serviços públicos, não houve uma lesão.

Importa saber então os tipos de hackers; para isso e necessário analisar classificação dada por Marcelo Crespo[104]: Dentre as nomenclaturas existentes, podemos citar:

> *a)Hackers*: Fuçador. Expressão que surgiu nos laboratórios do MIT (Massachussetts Institute of Technology). Qualquer um que tenha grande conhecimento sobre tecnologia e que faca invasões.
> *b) Carders:* Estelionatários especializados em fraudes com cartões.
> *c)Crackres:* Seriam os verdadeiros criminosos da rede. Utilizam seus conhecimentos de tecnologia para más finalidades.
> *d)Phreakers:* São os "hackers da telefonia", capazes de realizar interceptações, paralisar serviços e até mesmo utilizar a telefonia em nome de terceiros.

White Hat, em geral é um hacker do "bem" que tem como objetivo o aprendizado, não divulga os dados que manipula e lê; não é usual mas pode até exerce suas atividades à serviço de agências especializadas, delegacias, buscando por rastros daquele que adota uma conduta ilícita, apontando e corrige falhas. Usando tão somente seu conhecimento para boas ações. Nas palavras de Damásio de Jesus[105] os *White Hats* são "hackers éticos, especialistas que usam suas habilidades para o bem e fortalecimento da segurança dos sistemas".

Abaixo existe um exemplo de notícia com o "outro papel" desempenhado pelos Hackers, papel este aplaudido por grandes empresas uma vez que estes sujeitos apontam falhas técnicas e possibilidades de melhorias que muitas vezes passaram despercebidas por seus empregados, ou mesmo demorariam meses frente ao tempo que este profissional possa dedicar exclusivamente a esta empreitada, afinal geralmente são mais habilidosos, possuem um olhar "menos viciado" e vem nisso uma espécie de desafio com recompensas bem atrativas, ou seja "ao final há ainda um pote de ouro".

> Hackers faturam até US$ 700 mil por ano descobrindo bugs em sistemas
> REDAÇÃO OLHAR DIGITAL 02/05/2016 17H53 BUGHACKHACKERS
> Vistos por muita gente como vilões da internet, os hackers podem ajudar empresas a encontrar vulnerabilidades de segurança e consertá-las, antes que criminosos façam vítimas usando as falhas. A atividade, que

[104] CRESPO, Marcelo Xavier de Freitas. Crimes Digitais – São Paulo: Saraiva, 2011, p. 95
[105] JESUS, Damásio; MILAGRE, José Antônio. Manual de Crimes Informáticos. – São Paulo: Saraiva, 2016, p. 53.

> frequentemente é premiada pelas companhias, pode render uma pequena fortuna para quem faz disso sua profissão.
> É o caso de Jobert Abma, de 25 anos, fundador do HackerOne, um site onde as empresas podem pedir a hackers para serem atacadas e os recompensam pelos bugs encontrados. A página destaca pessoas para fazer o trabalho e fica com 20% do valor pago. O HackerOne oferece ainda um software que permite consertar as falhas encontradas.
> De acordo com o jovem, entre os 500 clientes estão empresas iniciantes, o Departamento de Defesa dos Estados Unidos, Twitter, Yahoo e até a Uber. Até abril, a empresa ajudou a pagar US$ 7 milhões a quem descobriu problemas em sistemas e sites.
> Mercado
> A HackerOne não é única empresa do setor. Bugcrowd, CrowdSecurity e SynAck são outros exemplos de gente que está ganhando muito dinheiro com bugs encontrados. "Há alguns hackers que conseguem ganhar US$ 200 mil por ano. Tem gente que tem como meta ganhar US$ 500 mil este ano", conta Abma.
> Trabalho
> Segundo ele, o dia de trabalho de um "hacker de recompensas" é igual ao de um profissional normal. "A maior parte deles trabalha com tecnologia, como engenheiros de software ou até profissionais da área de segurança. Eles usam isso como uma segunda fonte de renda. Somos pessoas normais, mas muito importantes para o futuro da internet", revela.[106]

Diferente dos hackers mencionados há outro tipo de sujeito ativo, este é definido como Black Hat, ou Cracker. É aquele que vale de seus conhecimentos para a prática de delitos; segundo Damásio[107], estes sim “são os verdadeiros criminosos da internet”. Algo próximo ao pensamento da autora Rita de Cássia:

> Ckacker é o invasor destrutivo que tenta invadir na surdina os portões de entrada dos serviços de internet, que são a melhor forma de disseminar informações. É o hacker malicioso, ou seja, possui grande conhecimento técnico e utiliza tal conhecimento para praticar crimes.

Conclui-se com esta classificação que o sujeito ativo, aquele que comete delitos na internet ou invade sistemas nem sempre foi um criminoso ou possuía pretensão de se tornar, podendo ser desde um usuário, aparentemente leigo, curioso, o qual não almejava qualquer uma destas condutas, mas graças as facilidades deste meio ganha encorajamento para fazer o que jamais faria no dia-a-dia. Portanto é incorreta a generalização de que todo hacker é um criminoso ou ainda que todo delito cometido no ciberespaço ou com o auxilio de um dispositivo informático será um cibercrime.

---

[106] http://olhardigital.uol.com.br/fique_seguro/noticia/hackers-faturam-até-us-700-mil-por-ano-descobrindo-bugs-em-sistemas/57851

[107] JESUS, Damásio; MILAGRE, José Antônio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016, p. 53.

4.4 TIPICIDADE OBJETIVA

Luiz Regis Prado[108] define Tipo Objetivo como os "caracteres objetivos do tipo (fato real que a lei proíbe). Comporta núcleo (verbo) e elementos secundários ou complementares".

Logo, para Vianna e Machado[109] o fato concentra-se nos verbos da ação de invasão/ instalação de vulnerabilidades em dispositivos informáticos ou qualquer outro capaz de processar dados.

> Os verbos típicos são *invadir* e *instalar* (vulnerabilidades). *Invadir* é a ação de acessar dados armazenados em dispositivos informáticos alheios, seja por meio da leitura, da escrita ou da execução.
> (...)
> O objeto material do delito são os dispositivos informáticos, isto é, computadores *desktop, notebooks, smartphones, tablets*, ou qualquer outro dispositivo capaz de processar dados automaticamente.
> *Instalar vulnerabilidades*, por sua vez, é a escrita e execução de *software* no dispositivo informático da vítima capaz de debilitar seus "mecanismos de segurança", de forma a viabilizar o acesso posterior pelo próprio agente ou por terceiro.

Essa é a mesma noção de tipo objetivo apresentada por Victor Gonçalves[110]:

> basta que o agente invada o computador alheio com o fim de obter, adulterar ou destruir dados ou informações, ou, ainda, que instale vulnerabilidades no sistema a fim de obter vantagem ilícita. Realizada uma dessas condutas, o delito estará consumado, ainda que o agente não atinja seu objetivo (obter, adulterar ou destruir informações ou obter vantagem ilícita). Em havendo um desses resultados posteriores, o fato poderá constituir crime mais grave.

Cumpre assim esclarecer algumas falhas do legislador. A primeira faz caracterizar como atípica a conduta quando o dispositivo invadido não dispor de obstáculos de segurança como senhas para restringir o acesso ou mesmo um antivírus; já que não houve então a invasão indevida, essa estava "aberta", como exemplifica Vianna e Machado[111].

> Trata-se, evidentemente, de uma lacuna grave na lei que não tutela os dados informáticos dos usuários inexperientes que não protegem suas maquinas com os tais "mecanismos de segurança.

---

[108] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro,** volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. – São Paulo: Revista dos Tribunais, 2013, p. 427
[109] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013. p.95.
[110] GONÇALVES, Victor Eduardo Rios. **"Direito penal esquematizado®**: parte especial - 6ed." iBooks. p.874 e 875.
[111] Ibid, p.96.

> (...)
> Um equivoco do legislador que não pode ser sanado pelo interprete em virtude da vedação à analogia in malam partem imposta pelo princípio constitucional da legalidade.

A segunda diz respeito a autorização do proprietário da máquina a um terceiro, que para o referido autor[112] também torna a conduta atípica.

> A autorização expressa é aquela formalizada por meio de um documento (impresso ou eletrônico) com assinatura (manual ou eletrônica) ou por qualquer outro registro da manifestação de vontade do titular do dispositivo. A autorização tácita e aquela fornecida por atos que demonstrem inequivocamente a permissão do titular dos dados para que o agente os acesse. Como por exemplo, pode-se citar o fornecimento de *login* de usuário e senha para um amigo. Ambos os tipos de autorização tornam a conduta atípica, mas a autorização tácita evidentemente exige uma prova em juízo mais complexa do que a simples apresentação de um documento de autorização expressa.

Por fim, existe ainda a previsão legal de que independe do dispositivo estar conectado ou não à Rede para que a conduta se caracterize.

Logo, o artigo 154-A define precisamente o comportamento de invasão e a instalação de vulnerabilidades, mas deixa passar despercebido três pontos que acarretaram em condutas atípicas; constituindo atitudes descobertas de uma persecução específica e portanto sem a eficácia esperada com a aplicação deste dispositivo.

4.5 TIPICIDADE SUBJETIVA

A definição de Tipo Subjetivo para Regis Prado[113] consiste nos caracteres subjetivos ou anímicos do tipo, do fato proibido por lei. Comporta o elemento subjetivo geral e eventualmente o elemento subjetivo do injusto.
Desta forma, como expõe Victor Goncalves[114], é necessário o dolo, o desejo por parte do agente em cometer o delito.

> É o dolo. Não existe modalidade culposa. Não há crime por parte de quem envia e-mail a outra pessoa sem saber que está transferindo um vírus ao outro aparelho. Note-se que a configuração da infração penal pressupõe a específica intenção de obter, adulterar ou destruir dados ou informações por meio da indevida invasão do dispositivo informático alheio, ou, ainda,

[112] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Forum, 2013, p. 96.
[113] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**, volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. – São Paulo: Revista dos Tribunais, 2013, p. 403.
[114] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado®** : parte especial – 6. ed. – São Paulo : Saraiva, 2016. – (Coleção esquematizado® / coordenação Pedro Lenza.), p. 877.

> de obter vantagem ilícita. Existe crime, por exemplo, por parte de quem invade computador de outrem com o intuito de danificar os arquivos existentes, de obter a senha de seu cartão bancário, de ter acesso ao conteúdo de suas conversas etc.

Assim, para Guilherme Nucci[115] não haverá punição para a conduta culposa, apenas para aquela cujo o fim esta previsto no tipo.

> Elemento subjetivo do tipo: é o dolo. Há elemento subjetivo do tipo específico para as duas condutas previstas no tipo. No tocante à invasão de dispositivo informático é o fim de obter, adulterar ou destruir dados ou informações. Focaliza-se a obtenção (ter acesso a algo), a adulteração (modificação do estado original) ou a destruição (eliminação total ou parcial) de dados (elementos apropriados à utilização de algo) ou informações (conhecimentos de algo em relação a pessoa, coisa ou situação). Quanto à instalação de vulnerabilidade é a obtenção de vantagem ilícita (qualquer lucro ou proveito contrário ao ordenamento jurídico). Pode ser, inclusive, a obtenção da invasão do dispositivo informático em momento posterior para obter dados e informações. Não se pune a forma culposa.

Adiante, Túlio Vianna e Felipe Machado[116], expõe que só e possível a modalidade culposa:

> O crime só é previsto na modalidade dolosa, O agente, portanto, deve ter consciência e vontade de praticar a ação típica. Caso se invada computador alheio, julgando ser próprio ou possuir a autorização para fazê-lo, incorre em erro típico, o que torna atípica a conduta por ausência do tipo subjetivo. Se o agente não pretendia invadir o dispositivo informático alheio, mas por imprudência, negligencia ou imperícia acaba por invadi-lo, não a que se falar em crime, pois não esta prevista a modalidade culposa deste delito. Pelo mesmo motivo não são puníveis os casos de erro de tipo neste crime. O tipo prevê ainda um "necessário "fim especial de agir" do autor que deve agir "com o fim de obter", adulterar ou destruir dados ou informações". SE o agente invade o dispositivo com finalidade jocosa, seja para enviar mensagem para a vítima ou mesmo para realizar alguma brincadeira como, por exemplo, abrir e fechar a gaveta do drive de DVD, a é atípica, por absoluta ausência do fim especial de agir.

Destarte, como no exemplo acima, caso o sujeito invada computador alheio julgando ser próprio ou por ter autorização de acesso, haverá erro do tipo, tornando atípica a conduta já que há ausência do tipo subjetivo (dolo) e além, espera-se um especial fim de agir, afinal quem incorre nesta modalidade tem como objetivo vantagens econômicas, obtenção de informações ou ainda a adulteração e destruição de dados. Consequentemente no artigo 154-A não há o que se falar sem que exista o dolo.

---

[115] NUCCI, Guilherme de Souza. **Código penal comentado.** 14. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2014, p. 1299.

[116] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013, p. 97.

4.6 CONSUMAÇÃO E TENTATIVA

a) Consumação

Regis Prado[117] conceitua consumação como a "realização de toda a ação descrita no conceito tipo; cogitação, preparação, execução e consumação". À vista disso Victor Gonçalves[118] define a consumação da invasão não autoriza a dispositivo informático como instantânea:

> No exato instante da invasão. Trata-se de crime formal que se consuma independentemente da efetiva obtenção, adulteração ou destruição de dados pretendida pelo agente. Na última figura do caput (instalar vulnerabilidades), o crime se consuma quando o arquivo espião é instalado, mesmo que o agente não consiga a vantagem pretendida.

Para Rogério Greco[119] o delito descrito no artigo 154-A também será formal; basta invadir o dispositivo ou instalar a vulnerabilidade para que se de a consumação.

> O delito tipificado no caput do art. 1 5 4-A se consuma no momento em que o agente consegue, efetivamente, invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, 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.
> Dessa forma, a obtenção, adulteração ou destruição dos dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou a instalação de vulnerabilidade para obtenção de vantagem ilícita, caso venham a ocorrer, devem ser consideradas como mero exaurimento do crime.

Túlio Vianna e Felipe Machado[120] observa que a consumação se dá com a invasão, mais precisamente com a leitura, qualquer conduta além incorre tão somente no exaurimento.

> O inicio da execução do crime se dá com a emissão do comando, ou da sequência de comandos destinados inequivocamente a acessar sem autorização o dispositivo informático alheio. A obtenção prévia de dados do

---

[117] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**, volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. – São Paulo: Revista dos Tribunais, 2013, p. 506.
[118] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado®** : parte especial – 6. ed. – São Paulo : Saraiva, 2016. – (Coleção esquematizado® / coordenação Pedro Lenza.), p. 877.
[119] GRECO, Rogério. GRECO, Rogério. **Curso de Direito Penal:** parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa - 11 . ed. Niterói, RJ: Impetus, 2015.p. 610.
[120] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Fórum, 2013, p. 98.

> agente, inclusive *login* e senha, constitui atos preparatórios não puníveis, desde que não sejam usados em qualquer tentativa de acesso.
> O crime se consuma com a leitura, escrita ou execução dos dados do sistema computacional.
> (...)
> O crime é material, pois exige um resultado para se consumar, pois não há invasão sem acesso ao menos de leitura aos dados.

Não há qualquer problema em entender a consumação do delito de invasão a dispositivos ou acesso a dados; basta imaginar que este é um segredo, como o outro delito do capitulo no qual insere-se o artigo 154-A, uma vez que este foi visto, lido, não importa se será revelado ou vendido para que tenha sido violado, isso aconteceu no exato instante de sua descoberta.

b) Tentativa:

A tentativa para Regis Prado[121] vem a ser um "tipo incompleto, no qual o tipo subjetivo esta perfeito, mas o tipo objetivo não se perfaz integralmente, uma vez que falta o atributo material, sendo portanto defeituoso, mas por circunstâncias alheias a vontade do autor."

Ao passo que Victor Goncalves[122] admite a tentativa. "É possível. É o que ocorre, por exemplo, quando a vítima não abre um e-mail que lhe foi enviado (spam) contendo arquivo espião ou quando o programa antivírus impede uma invasão."

Exaustivamente, Túlio Vianna e Felipe Machado[123] concluem que a invasão de dispositivo informático não autorizada constitui crime material, exigindo-se então um resultado; o qual inicia-se com a emissão dos comando para acessar o dispositivo, mas vem a concluir apenas com a leitura, execução dos dados. E todo o conjunto de ações antecedentes, como a obtenção de *login*, senha nada mais são que atos preparatórios, os quais não podem ser puníveis. Isto faz cair por terra a defesa da tese de que esta conduta seria formal, consumando-se inclusive sem a obtenção dos dados; o que constitui uma confusão do tipo subjetivo com o objetivo.

Como pode ser analisado abaixo:

---

[121] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**, volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. São Paulo: Revista dos Tribunais, 2013, p. 508.
[122] GONÇALVES, Victor Eduardo Rios. "**Direito penal esquematizado®:** parte especial - 6ed." iBooks. p.878
[123] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informativos.** Belo Horizonte: Forum, 2013, p. 98.

> É admissível, portanto, a tentativa quando, após iniciada a execução, o crime não se consuma por circunstancias alheia á vontade do agente como, por exemplo, uma queda repentina de energia elétrica ou de sinal de Internet.

Uma vez que a conduta é material, e necessita do acesso aos dados, se após efetivado o ingresso o agente destruir tais informações o crime exaure-se da mesma maneira pois já havia sido consumado.

4.7 SANÇÃO PENAL E ASPECTOS PROCESSUAIS PENAIS

Para Regis Prado[124] a Ação Penal é o momento da persecução do crime no qual se concretiza a acusação contra seu autor.

Ela pode ser pública, e portanto tem o MP como titular; e divide-se em: condicionada, isto é, dependente da representação do ofendido ou da requisição do Ministro da Justiça; ou Incondicionada, e portanto independe de representação do ofendido ou de requisição do Ministro da Justiça para sua proposição. No caso do Art. 154-A Victor Goncalves[125] dispõe que em regra a ação será pública e condicionada, salvo nos casos em que o bem jurídico violado for público.

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

O que é ratificado por Guilherme Nucci[126]:

> É pública condicionada à representação, como regra. Entretanto, há figuras típicas inadequadas a tal disposição, como já mencionamos ao comentar o § 1.º do art. 154-A.
> A produção, oferecimento, distribuição, venda ou difusão de dispositivo ou programa de computador que possa permitir a invasão a dispositivo informático não tem vítima determinada. Interessa à sociedade a sua punição, impedindo-se que chegue a violar dados de alguém. No entanto, constituindo crime de ação pública condicionada à representação, inexiste quem possa fazê-lo. A única hipótese viável seria encontrar a pessoa ofendida pela conduta do caput, que se seguiu à do § 1.º De outra parte, se o crime for cometido contra a administração pública direta ou indireta de

[124] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro**, volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. São Paulo: Revista dos Tribunais, 2013, p. 857.
[125] GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado®** : parte especial - 6ed." iBooks. p. 884.
[126] NUCCI, Guilherme de Souza. **Código penal comentado.** 14. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2014, p. 1306.

> qualquer dos Poderes da República ou empresas concessionárias de serviços públicos a ação é pública incondicionada.

Para Vianna e Machado[127]

> Nos termos do art. 154-B do CPB, quando o crime for cometido contra a "administração pública direita ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionarias de serviços públicos", a ação penal será pública incondicionada. Nessa hipótese, possível é a aplicação dos institutos da transação penal (art. 76 da Lei n.º 9.099/95) e se, não atendidos algum de seus requisitos como, por exemplo, o agente té-lo utilizado em menos de 5 anos, cabível ainda será a suspensão condicionada do processo, prevista no art. 89, da mesma lei.
> Por outro lado, se o crime não for cometido contra os sujeitos passivos acima narrados, a ação penal será pública, mas condicionada à representação do ofendido. Aqui, para além da transação penal e da suspensão condicional do processo, também há a possibilidade da composição civil do dano (art. 60, paragrafo único, da Lei n.º 9.099/95), acordo este que, se homologado pelo juiz em sentença irrecorrível acarreta renuncia ao direito de representação (art. 74, parágrafo único, da Lei n.º 9.099/95)

Por oportuno deve ser levantado o questionamento a cerca da efetividade desta persecução penal. Existe a tipificação da conduta? Sim. Ela é efetiva? Depende. Para um criminoso que invadiu o dispositivo de um indivíduo, publicou informações importantes, ou fotos e ainda possa valer-se de seus documentos para cometer outras atrocidades no futuro, a transação penal, ou ainda 5 anos de condenação e indenização (multa) não farão que o dano seja restaurado, que a imagem do cidadão ou de sua empresa seja refeita (nos casos de difamação). Mas em contrapartida o simples ato de temporariamente interromper o funcionamento de um site, sem qualquer outra finalidade, não pode ser razão para cercear a liberdade de um indivíduo.

Sem mencionar as causa de aumento de pena, ainda assim é evidente a discrepância, principalmente ao analisar que uma vez que o indivíduo venha a ser condenado isso não ira impedir que ele retorne a cometer estes crimes, sobretudo nos casos de vantagem econômica, que é muito superior a condenação.

Os lucros possíveis e o tempo para que localize este sujeito, em razão das limitações de investigação possibilita que nesse lapso temporal um alto número de pessoa se torne vítimas até que qualquer pena tenha efeito.

---

[127] VIANNA, Túlio; MACHADO, Felipe. **Crimes Informativos**. Belo Horizonte: Fórum, 2013, p. 100.

5 CONSIDERAÇÕES FINAIS

No presente trabalho, foram levantadas duas importantes questões: existe tipificação para os cibercrimes? Ela é eficaz? Inicialmente fica claro que há uma evolução da sociedade; tanto do homem como das tecnologias que o cerca; desenvolvimento este que não é acompanhado com a legislação pátria. O que contribui diretamente na forma como o indivíduo se porta e consequentemente na evolução criminal.

Uma vez que a Internet evoluiu e derrubou fronteiras fez nascer para alguns a sensação de que praticar um delito é extremamente simples, e não bastasse isso por vezes há a impunidade ou ainda que a punição ocorra aparenta existir mais vantagens no cometimento do delito. No jargão da esfera criminal “ainda que o indivíduo caia não da nada, ele pagará umas cestas básicas, ou no máximo em um aninho estará solto”. Frente a este pensamento é complicado defender que realmente por alguns milhões não valeriam a pena vazar o conteúdo de um computador que estava ali a sua frente.

Além disso a própria evolução coopera, ao tornar-se um mecanismo para a prática de crimes e de condutas lesivas a diversos bens jurídicos nas mãos de sujeitos mal intencionados. Pois com seu aprimoramento, houve a melhora dos métodos utilizados para cometer tais delitos; existe a simplificação das formas para cometer o delito, sem que haja a necessidade de um contato direto, de um exposição acentuada ou mesmo a espera por um momento ideal.

Ao mesmo tempo que há o acesso ao um maior número de vítimas, sendo muitas dessas relapsas, descuidas ou desprovidas de esclarecimento suficiente para se proteger, existe a polícia, que não possui ainda todo o efetivo, os requisitos, todas as ferramentas, o conhecimento necessário e a disponibilidade de tempo para verificar estas situações. Muitas vezes quando é sabido do delito já é tarde e o criminoso encontrou meios para apagasse seus rastros.

Isso tudo faz com que muitas das vítimas não busque a garantia de seus direitos, ou acabem por ceder as exigências do criminoso, ao julgar encontrar uma solução mais rápida; deixando estes sujeitos impunes mesmo diante que tenham cometido atos inescrupulosos perante a sociedade.

O potencial de alguns deste crimes podem desgraçar a vida da vítima, fazer com que ela perca o emprego, que sua empresa tenha sua credibilidade e

rendimentos afetados e vários outros danos que nenhuma punição existente até o momento será eficaz, tampouco suficiente para restaurar tudo o que foi perdido, toda a lesão.

Por isso é imperativo que esse tanto de conhecimento e avanços tecnológicos, atinjam e venham a ser aproveitados pela Justiça para realizar com competência o combate à criminalidade, em benefício dela e de toda a sociedade.

Apesar de nos últimos anos muito se ter estudado acerca dos cibercrimes, de propor modificações legais acerca do tratamento que deve ser aplicado as condutas possíveis na Internet ou por meio de dispositivos informáticos e aos agentes praticantes dela, pouco foi construído, e o que foi carece ainda de efetividade.

São décadas de projetos, razoáveis, mas que foram discutidos sem um norte ou que as melhores propostas se perderam. Sendo fruto delas apenas três leis, que auxiliaram sim na proteção de alguns bens jurídicos e tipificaram condutas. Mas cujo texto legal foi mal elaborado, contém pontos desatualizados e deixou de especificar tais institutos com o tamanho rigor que era necessário.

Diante desse estudo é possível afirmar que o legislador começou a acertar ao buscar a proteção dos dados só que abundam falhas. Impera a ele corrigir lacunas acerca da propriedade do dispositivo, da autorizações de uso do dispositivo, de condutas que foram classificadas como atípicas e outros pormenores.

Aquém, como forma de evitar os delitos e proporcionar ao cidadão mais segurança é imprescindível o investimento em educação. Esse mecanismo e denominado prevenção primária, ele busca coibir a cogitação delitiva, isto é, a propagação de uma cultura que ser criminoso pode ser bom, que ser um hacker (na verdade cracker) é algo vantajoso e possibilita o enriquecimento sem qualquer punição.

É preciso que haja educação no tocante a como as pessoas se expõe na Internet, como é fácil conhecer tudo sobre ela, inclusive prováveis senhas apenas com o acesso suas redes sociais. Para que assim, ela mesma tenha uma proteção alternativa com forma de manter a sua liberdade. E assim possa agir como bem entender mas sem se por em situações de risco.

Outro ponto importante é a prevenção secundária. Na qual o Estado estuda como são os crimes, realiza um levantamento do índices e analisa de que forma se

dão para então tentar suprimir aquilo que torne o propício.

Porque ainda que a internet seja por si só um ambiente de risco, como defende a Ministra Nancy Andrighi, isso não retira de cada cidadão o direto de poder agir como desejar, de ter a garantia da sua liberdade, privacidade e o oportunidade de se expressão. É mister que assim como se deu o acolhimento da Internet como direito fundamental, o governo propicie meios de torná-la mais segura.

Uma solução que já tem sido adotada paliativamente é a adaptação. Ainda que o crescimento da Internet seja algo descomedido os operadores do direito precisam tentar enquadrar as práticas cometidas neste meio, ou com a utilização de dispositivos eletrônicos, nos tipos penais existentes já que não entra em vigor uma legislação no mesmo tempo de sua necessidade.

Por fim, ressalva-se também, que as próximas leis a serem criadas carecerão de cuidados para que não contenha termos, condutas que a torne obsoleta tão rapidamente.

O presente trabalho se firmou em apresentar de forma graduada, as teses, problemas, soluções, pretensões, responsabilidades, sujeitos, e histórico de um assunto de suma importância. Sabe-se que a questão dos crimes Cibernéticos não se esgotou como tema de discussões atuais, ainda não apresenta um estudo bem definido, todavia, espera-se que a leitura deste trabalho alcance os objetivos pretendidos, só assim este estudo se realizará por completo.

6 REFERÊNCIAS

AZEVEDO, Ana. **Marco Civil da Internet no Brasil.** Rio de Janeiro: Alta Books, 2014.

BRASIL. Constituição da República Federativa do Brasil de 1988.

_____. **Código Penal.** Decreto-lei n. 2.848, de 7 de dezembro de 1940.

_____. **Lei nº 12.735,** de 30 de novembro de 2012.

_____. **Lei nº 12.737**, de 30 de novembro de 2012.

_____. **Lei nº 12.965,** de 23 de abril de 2014.

CAPEZ, Fernando. **Código penal comentado.** 3. ed. São Paulo : Saraiva, 2012. 1. Direito penal - Legislação - I. Título.

_____. **Curso de Direito Penal**, volume 2, parte especial: dos crimes contra a pessoa e dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212) – 15. Ed. – São Paulo: Saraiva, 2015

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado:** parte especial – 6. ed. – São Paulo : Saraiva, 2016. (Coleção esquematizado / coordenação Pedro Lenza.)

GRECO, Rogério. **Curso de Direito Penal:** parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa - 11 . ed. Niterói, RJ: Impetus, 2015.

JESUS, Damásio de. **Manual de crimes informático.** São Paulo: Saraiva, 2016

KANAAN, João Carlos. **Informática global: tudo o que você precisa saber sobre informática.** São Paulo: Pioneira, 1998.

MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet.** São Paulo: Ed. RT, 2008.

NUCCI, Guilherme de Souza. **Código penal comentado.** 15. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2015.

_____. **Código penal comentado.** 14. ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2014.

_____. **Código Penal: Comentado.** 13. ed.. Rio de Janeiro - RJ: Forense, 2013. 774 p. il. revista, atualizada e ampliada.

OLIVEIRA, José Nicodemos Vitoriano de. **Internet como direito fundamental.** Revista Jus Navigandi, Teresina, ano 18, n. 3533, 4 mar. 2013. Disponível em: <https://jus.com.br/artigos/23867>. Acesso em: 9 jun. 2016.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro,** volume 1: parte geral, art. 1 a 120. 12ed. Rev. Anul. E ampl. – São Paulo: Revista dos Tribunais, 2013

SCHERKERKEWITZ, Iso Chaitz. **Direito e Internet.** São Paulo: Editora Revista dos Tribunais, 2014.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 20. ed. São Paulo: Malheiros, 2001.

SILVA, Rita de Cássia Lopes da. **Direito Penal e sistema informático**. São Paulo: Editora Revista dos Tribunais, 2003.

SKINNER, Burrhus Fredcric, 1904-1990. **Ciência e comportamento humano** / B. F. S kinner; tradução João Carlos Todorov, Rodolfo Azzi. – 1. ed. - São Paulo: Martins Fontes, 2003. - (Coleção biblioteca universal)

SYDOW, Spencer Toth. **Crimes Informáticos e suas vítimas.** 2ed. – São Paulo: Saraiva, 2015

TAKAHASHI, Tadao (Org.). **Sociedade da Informação no Brasil:** Livro verde. Brasília. Ministério da Ciência e Tecnologia, 2000.

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

WENDT, Emerson.; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2ed. - Rio de Janeiro: Brasport, 2013.

http://www.internetlivestats.com/internet-users/ >. Acesso em 18.05.2016 as 04h12
http://www.internetworldstats.com/stats2.htm - Acesso em 12.06.2016 as 15h55.

http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html >. Acesso em 12.06.2016 as 15h55

http://erickcordeiro.jusbrasil.com.br/artigos/318501353/o-alcance-juridico-na-deep-web?ref=topic_feed >. Acesso em 07.05.2016 as 01h37

http://www.itamaraty.gov.br/pt-BR/component/tags/tag/90-direito-a-privacidade-na-era-digital >. Acesso em 07.06.2016 as 21h22

https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais >. Acesso em 08.06.2016 as 00h37

https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais >. Acesso em 11.06.16 as 20h55

http://olhardigital.uol.com.br/fique_seguro/noticia/brasil-e-um-dos-10-paises-onde-mais-surgem-virus-de-computador/57806 >. Acesso em 30.04.2016 as 16h58

http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf >. Acesso em 12.06.16 as 01h01

http://olhardigital.uol.com.br/fique_seguro/noticia/hackers-faturam-até-us-700-mil-por-ano-descobrindo-bugs-em-sistemas/57851 >. Acesso 03.05.16 as 16h47

http://www.istoedinheiro.com.br/blogs-e-colunas/post/20160506/brasil-grande-produtor-virus/8824. Acesso 12.06.2016 as 18h07.

http://www3.pucrs.br/pucrs/files/uni/poa/direito/graduacao/tcc/tcc2/trabalhos2007_1/ivar_hartmann.pdf >. Acesso em 09.06.16 as 17h32

ANEXOS

Anexo I

Jurisprudências

DIREITO PROCESSUAL PENAL. COMPETÊNCIA PARA PROCESSAR E JULGAR OS SUPOSTOS RESPONSÁVEIS PELA TROCA DE MENSAGENS DE CONTEÚDO RACISTA EM COMUNIDADES DE REDE SOCIAL NA INTERNET. Ainda que os possíveis autores dos fatos criminosos tenham domicílio em localidades distintas do território nacional, compete ao juízo do local onde teve início a apuração das condutas processar e julgar todos os supostos responsáveis pela troca de mensagens de conteúdo racista em comunidades de rede social na internet, salvo quanto a eventuais processos em que já tiver sido proferida sentença. Em situações como essa, embora cada mensagem constitua crime único, existe conexão probatória entre os processos instaurados para a apuração das condutas. A circunstância na qual os crimes teriam sido praticados – troca de mensagens em comunidade virtual – estabelece uma relação de confiança, ainda que precária, entre os usuários, cujo viés pode facilitar a identificação da autoria. Com efeito, ao ingressar em uma comunidade virtual, o usuário tem a expectativa de que os demais membros compartilhem da sua opinião. Dessa maneira, não é incomum que o vínculo estabelecido vá além da mera discussão, propiciando uma autêntica troca de informações, inclusive pessoais, entre os usuários desse espaço. Ademais, é a forma por meio da qual os membros interagem na comunidade virtual que cria o nexo entre as mensagens que ali circulam e, consequentemente, estabelece um liame entre as condutas supostamente ilícitas. Assim, embora a competência para processar e julgar o crime de racismo praticado por meio da internet se estabeleça de acordo com o local de onde partiram as manifestações tidas por ofensivas, o modus operandi consistente na troca de mensagens em comunidade virtual deve ser considerado como apto a caracterizar a conexão probatória (art. 76, III, do CPP). Portanto, constatada a suposta ocorrência de crimes conexos, a competência deve ser fixada pela prevenção, em favor do juízo no qual as investigações tiveram início, com ressalva apenas quanto a eventuais processos em que já tenha sida proferida a sentença. Com efeito, de acordo com o disposto no art. 82 do CPP, se, “não obstante a conexão ou continência forem instaurados processos diferentes, a autoridade de jurisdição prevalente deverá avocar os processos que corram perante os outros juízes, salvo se já estiverem com sentença definitiva”. Ainda acerca desse ponto, deve ser mencionada a Súmula 235 do STJ, segundo a qual a “conexão não determina a reunião dos processos, se um deles já foi julgado”. Precedente citado: CC 102.454-RJ, DJe 15/4/2009. CC 116.926-SP, Rel. Min. Sebastião Reis Júnior, julgado em 4/2/2013.

E M E N T A: EXTRADIÇÃO – PRISÃO CAUTELAR – PLEITO FORMULADO PELA INTERPOL – POSSIBILIDADE – INOVAÇÃO INTRODUZIDA PELA LEI Nº 12.878/2013 – DELITO INFORMÁTICO (CRIME DIGITAL): “INVASÃO DE DISPOSITIVO INFORMÁTICO” (CP, ART. 154-A, ACRESCIDO PELA LEI Nº 12.737/2012)– FATO DELITUOSO ALEGADAMENTE COMETIDO, EM TERRITÓRIO AMERICANO (ESTADO DO TEXAS), EM 2011 – CONDUTA QUE, NO MOMENTO EM QUE

PRATICADA (2011), AINDA NÃO SE REVESTIA DE TIPICIDADE PENAL NO ORDENAMENTO POSITIVO BRASILEIRO – O SIGNIFICADO JURÍDICO DO PRINCÍPIO CONSTITUCIONAL DA RESERVA DE LEI EM MATÉRIA DE TIPIFICAÇÃO E DE COMINAÇÃO PENAIS (CF, ART. 5º, INCISO XXXIX)– "NULLUM CRIMEN, NULLA POENA SINE PRAEVIA LEGE" – DUPLA TIPICIDADE (OU DUPLA INCRIMINAÇÃO): CRITÉRIO QUE REGE O SISTEMA EXTRADICIONAL – NECESSIDADE DE QUE O FATO SUBJACENTE AO PEDIDO DE EXTRADIÇÃO (OU AO PLEITO DE PRISÃO CAUTELAR PARA EFEITOS EXTRADICIONAIS) ESTEJA SIMULTANEAMENTE TIPIFICADO, NO MOMENTO DE SUA PRÁTICA, TANTO NA LEGISLAÇÃO PENAL DO BRASIL QUANTO NA DO ESTADO ESTRANGEIRO – PRECEDENTES – SITUAÇÃO INOCORRENTE NO CASO, POIS A CONDUTA PUNÍVEL IMPUTADA AO SÚDITO ESTRANGEIRO RECLAMADO SOMENTE PASSOU A SER CONSIDERADA CRIMINOSA, NO BRASIL, EM ABRIL DE 2013 (QUANDO SE ESGOTOU O PERÍODO DE "VACATIO LEGIS" DA LEI Nº 12.737/2012, ART. 4º), POSTERIORMENTE, PORTANTO, À DATA EM QUE FOI ELA ALEGADAMENTE PRATICADA NOS ESTADOS UNIDOS DA AMÉRICA – EVOLUÇÃO DO TRATAMENTO LEGISLATIVO, NO BRASIL, PARA FINS PENAIS, DOS CRIMES INFORMÁTICOS – OCORRÊNCIA, AINDA, NA ESPÉCIE, DE OUTRO OBSTÁCULO JURÍDICO: DELITO INFORMÁTICO (OU CRIME DIGITAL, OU INFRAÇÃO PENAL CIBERNÉTICA) SEQUER PREVISTO NO ARTIGO II DO TRATADO DE EXTRADIÇÃO BRASIL/EUA – ROL EXAUSTIVO, FUNDADO EM "NUMERUS CLAUSUS", QUE DEFINE, NO CONTEXTO BILATÉRAL DAS RELAÇÕES EXTRADICIONAIS ENTRE BRASIL E EUA, OS CRIMES QUALIFICADOS PELA NOTA DE "EXTRADITABILIDADE" – PRECEDENTES, A ESSE RESPEITO, DO SUPREMO TRIBUNAL FEDERAL – CONSEQUENTE IMPOSSIBILIDADE DE PROCESSAR-SE DEMANDA EXTRADICIONAL FUNDADA EM DELITO ESTRANHO AO ROL TAXATIVO INSCRITO NO ARTIGO II DESSE TRATADO DE EXTRADIÇÃO – NATUREZA JURÍDICA DO TRATADO DE EXTRADIÇÃO ("LEX SPECIALIS") – PRECEDÊNCIA JURÍDICA, QUANTO À SUA APLICABILIDADE, SOBRE O ORDENAMENTO POSITIVO INTERNO DO BRASIL – "PACTA SUNT SERVANDA" – PRECEDENTES – A INADMISSIBILIDADE DA EXTRADIÇÃO (CAUSA PRINCIPAL) TORNA INVIÁVEL O ATÉNDIMENTO DO PEDIDO DE PRISÃO PREVENTIVA (MEDIDA REVESTIDA DE CAUTELARIDADE E IMPREGNADA DE CARÁTER ANCILAR E MERAMENTE ACESSÓRIO) – QUESTÃO DE ORDEM QUE SE RESOLVE NO SENTIDO DO INDEFERIMENTO DO PEDIDO DE PRISÃO CAUTELAR.

(STF - PPE: 732 DISTRITO FEDERAL 9999906-02.2014.1.00.0000, Relator: Min. CELSO DE MELLO, Data de Julgamento: 11/11/2014, Segunda Turma, Data de Publicação: 02/02/2015)

PENAL. PROCESSO PENAL. RECURSO EM SENTIDO ESTRITO. APROPRIAÇÃO INDÉBITA

. INVASÃO DISPOSITIVO INFORMÁTICO. CRIMES DE AÇÃO PÚBLICA INCONDICIONADA E CONDICIONADA À REPRESENTAÇÃO.

> MINISTÉRIO PÚBLICO. TITULARIDADE. LEGITIMIDADE. INÉRCIA NÃO DEMONSTRADA. NÃO INCIDÊNCIA DO ARTIGO 29, DO CPP. 1 - Cabe privativamente ao Ministério Público a promoção das ações penais públicas incondicionadas ou condicionadas à representação, nos termos do artigo 129, inciso I, da Constituição Federal. 2 - Correta a decisão que rejeita a queixa por crimes previstos nos artigos 168 e 154-A, ambos do CP, diante da ausência de condição para o exercício da ação penal privada, consubstanciada na ilegitimidade ativa do particular para promover a persecutio criminis. 3. A ação penal privada, subsidiária da pública, somente é cabível nas hipóteses de manifesta inércia do dominus litis, consoante exegese do artigo 29, do Código de Processo Penal. 4 - Recurso conhecido e desprovido.
>
> (TJ-DF - RSE: 20151410060384, Relator: SANDOVAL OLIVEIRA, Data de Julgamento: 10/03/2016, 3ª Turma Criminal, Data de Publicação: Publicado no DJE : 14/03/2016 . Pág.: 176)

Recurso em sentido estrito. Crimes de injúria, ameaça e invasão de dispositivo informático. Declaração de incompetência. Remessa dos autos ao JECRIM. Acolhimento da preliminar suscitada pelo órgão ministerial. Queixa-crime ofertada em face de delitos promovidos mediante ação penal pública condicionada a representação. Ausência de inércia do Ministério Público. Rejeição, de ofício, da queixa-crime no tocante aos delitos previstos no artigo 147 e 154-A, ambos do Código Penal. Procuração que não atende os requisitos do artigo 44 do Código de Processo Penal. Ausência de poderes especiais ao procurador, indicação do nome do querelado, bem como de menção ao fato supostamente criminoso. Vício sanável dentro do prazo decadencial. Transcuro do prazo decadencial. Declaração, de ofício, da extinção da punibilidade do querelado. Recurso improvido. (TJ-SP - RSE: 00015189320158260650 SP 0001518-93.2015.8.26.0650, Relator: Leme Garcia, Data de Julgamento: 22/03/2016, 16ª Câmara de Direito Criminal, Data de Publicação: 23/03/2016)

Anexo II

Presidência da República Casa Civil Subchefia para Assuntos Jurídicos

LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.

Mensagem de veto
Vigência

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

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

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

Art. 2º (VETADO)

Art. 3º (VETADO)

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

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

“Art. 20. .....

§ 3º .....

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

....." (NR)

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

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

DILMA ROUSSEFF

José Eduardo Cardozo

Paulo Bernardo Silva

Maria do Rosário Nunes

Este texto não substitui o publicado no DOU de 3.12.2012

*

Anexo III

Presidência da República Casa Civil Subchefia para Assuntos Jurídicos

LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Vigência

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

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

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

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

"Invasão de dispositivo informático

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

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

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

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

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

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

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver

divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

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

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

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

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

"Ação penal

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

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

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

Art. 266. .....

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

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

"Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

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

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

sua publicação oficial.

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

DILMA ROUSSEFF

José Eduardo Cardozo

Este texto não substitui o publicado no DOU de 3.12.2012

Anexo IV

Presidência da República - Casa Civil - Subchefia
para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Vigência

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

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

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

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

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

I - o reconhecimento da escala mundial da rede;

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

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

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

VI - a finalidade social da rede.

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

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

II - proteção da privacidade;

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

IV - preservação e garantia da neutralidade de rede;

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

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

VII - preservação da natureza participativa da rede;

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

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

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

I - do direito de acesso à internet a todos;

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

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

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

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

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

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

V - manutenção da qualidade contratada da conexão à internet;

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

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

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

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I

Da Neutralidade de Rede

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

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê

Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

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

II - priorização de serviços de emergência.

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

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

II - agir com proporcionalidade, transparência e isonomia;

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

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

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

Seção II

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

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

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

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

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que

informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

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

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

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

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

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

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

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

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

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

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

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

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

Subseção I

Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II

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

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

Subseção III

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

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

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

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

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

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os

registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

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

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

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

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

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

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

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à

indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

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

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

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

Seção IV

Da Requisição Judicial de Registros

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

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

I - fundados indícios da ocorrência do ilícito;

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

III - período ao qual se referem os registros.

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

pedidos de guarda de registro.

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

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

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

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

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

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

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

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

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

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

IX - promoção da cultura e da cidadania; e

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

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

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

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais

e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

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

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

V - fortalecimento da participação social nas políticas públicas.

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

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

I - promover a inclusão digital;

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

III - fomentar a produção e circulação de conteúdo nacional.

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

CAPÍTULO V

DISPOSIÇÕES FINAIS

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

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no**caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

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

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19,

a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

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

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

Miriam Belchior

Paulo Bernardo Silva

Clélio Campolina Diniz

Este texto não substitui o publicado no DOU de 24.4.2014.