UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE NACIONAL DE DIREITO

O CRIME DE FURTO E SUAS IMPLICAÇÕES NO MEIO CIBERNÉTICO:

LEGALIDADE E DIFERENÇAS QUANTO AOS BENS JURIDÍCOS TUTELADOS

JEAN MARTINS RIBEIRO

Rio de Janeiro
2018.1

JEAN MARTINS RIBEIRO

O CRIME DE FURTO E SUAS IMPLICAÇÕES NO MEIO CIBERNÉTICO:

LEGALIDADE E DIFERENÇAS QUANTO AOS BENS JURIDÍCOS TUTELADOS

Monografia de final de curso, elaborada no âmbito da graduação em Direto da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação da Professora Fernanda Prates Fraga.

Rio de Janeiro
2018.1

CIP - Catalogação na Publicação

Ribeiro, Jean Martins
R484c O crime de furto e suas implicações no meio cibernético: legalidade e diferenças quanto ao bens jurídicos tutelados / Jean Martins Ribeiro. -- Rio de Janeiro, 2018.
64 f.

Orientadora: Fernanda Prates Fraga.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2018.

1. Crime de furto e suas nuances no meio cibernético. 2. Lei 12.737/12 aspectos gerais e críticas. 3. Legalidade e crime digital . I. Fraga, Fernanda Prates, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

JEAN MARTINS RIBEIRO

O CRIME DE FURTO E SUAS IMPLICAÇÕES NO MEIO CIBERNÉTICO:

LEGALIDADE E DIFERENÇAS QUANTO AOS BENS JURIDÍCOS TUTELADOS

Monografia de final de curso, elaborada no âmbito da graduação em Direto da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação da Professora Fernanda Prates Fraga.

Data da Aprovação: __ / __ / ____

Banca Examinadora:

_____
Orientador

_____
Co-orientador (Opcional)

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro
2018.1

DADOS PESSOAIS

Jean Martins Ribeiro

DRE: 113138978

Telefone: + 55 (21) 2464-0885

Celular: + 55 (21) 98409-9090

E-mail: jean.martins94@hotmail.com

Ed.: Rua Barão,1173, casa 32. Praça Seca - Jacarepaguá. RJ

CEP: 21.321-620

Turno: Integral

Orientadora: Fernanda Prates Fraga

AGRADECIMENTOS

Agradeço à minha família por sempre ter me apoiado. Ione, Remi, Renan, e Roberta, meu Norte.

Cada qual sabe amar a seu modo; o modo, pouco importa; o essencial é que saiba amar

Machado de Assis

RESUMO

A presente monografia trata dos aspectos dos aspectos mais relevantes do crime de furto e da conduta tratada como furto de dados, passando por todos os pontos que os diferenciam e os conectam, sendo esses: o bem jurídico tutelado; legalidade dos tipos penais e interpretação da lei penal; decisões recentes sobre o assunto; leis que dispõem sobre a temática e críticas a essas; e o agente de cada um deles. Ressalta a necessidade de implementação de legislação apropriada para solucionar todos os questionamentos presentes na problemática, desde a inexpressividade da lei 12.737/12 até a atipicidade do crime de furto quando perpetrado pelo meio cibernético.

Palavras-Chaves: Direito Penal; Crime de furto; Furto de dados; Principio da Reserva Legal; Lei 12.737/12.

ABSTRACT

This monograph deals with aspects of the most relevant aspects of the crime of theft and of the conduct treated as data theft, going through all the points that differentiate them and connect them, these being: the legal good protected; legality of criminal offenses and interpretation of criminal law; recent decisions on the subject; laws on the subject and criticism of them; and the agent of each of them. It stresses the need to implement appropriate legislation to solve all the questions present in the problematic, from the inexpressiveness of Law 12.737/12 to the atypical crime of robbery when perpetrated by the cybernetic medium

Keywords: Criminal Law; Crime of theft; theft of data; Principle of Legal Reserve; Law 12.737/12.

SUMÁRIO

INTRODUÇÃO 8
1 HISTÓRIA E EVOLUÇÃO DIGITAIS 13
1.1 HISTÓRIA DA INTERNET 13
1.2 CENÁRIO DOS DANOS CAUSADOS NO MEIO CIBERNÉTICO 17
2 O MECANISMO DO CRIME CIBERNÉTICO 24
2.1 DIREITO À PRIVACIDADE 24
2.2 JURISDIÇÃO DIGITAL 25
2.3 O AGENTE DO CRIME 28
3 CRIME DE FURTO E A LEGALIDADE 35
3.1 FURTO 35
3.2 CRIMES DIGITAIS PUROS OU MISTOS 38
3.3 DA LEGALIDADE 40
4 DA LEGISLAÇÃO PERTINENTE 42
4.1 LEI 12.737/12 42
4.2 CRÍTICAS À LEI 12.737/12 50
CONSIDERAÇÕES FINAIS **54**
REFERÊNCIAS BIBLIOGRÁFICAS **60**

INTRODUÇÃO

Com o advento da internet e o desenvolvimento das tecnologias e dispositivos eletrônicos que permitem acesso a ela pelos usuários, como smartphones, aplicativos, wi-fi, e-mail, dentre outros, houve a possibilidade de ser feito compartilhamento de dados, como meio de propagação de informações e de comunicação.

Tudo isso, em um contexto de aceleração do ritmo nas mudanças de como se entende as relações entre as pessoas de todo o mundo, com grande integração e flexibilidade, denominado "globalização". Surge, então, a problemática da criminalidade nesse âmbito, que passa a fazer parte da realidade dessa esfera, da rede mundial de computadores e seus integrantes.[1]

Bens jurídicos, que antes não eram afetados por este meio (ou talvez nem mesmo existissem), agora são. O Estado, que antes abrangia os anseios da sociedade em tutelar seus bens jurídicos, agora se vê em xeque, diante do questionamento da necessidade de adaptação, reformulação ou não do seu ordenamento jurídico.

O presente trabalho pretende tratar do tema a partir, não do advento da computação ou internet em si, mas do momento em que o Brasil passou a ter o tema como de relevante valor para grande parcela de sua população, com maior acesso à grande rede mundial de computadores, e coincidentemente a Constituição da República Federativa do Brasil de 1988 passou a vigorar em seu em seu território.[2]

Para tal, serão tratados, a partir da data supramencionada, decisões diversas instâncias do ordenamento jurídico brasileiro, até chegar às das Cortes Superiores e do Supremo Tribunal Federal pertinentes, além de comentários jurídicos ligados a elas e doutrinas que tratem de conceitos basilares e fundamentadores, tratativa sobre a

---

[1] TANGERINO, Dayane Fanti. "Direito Penal e Novas Tecnologias". **Canal Ciências Criminais**. Jan. 2016. Disponível em: <https://canalcienciascriminais.com.br/direito-penal-e-novas-tecnologias/>. Acesso em: mar. 2018.

[2] TANGERINO, Dayane Fanti. "Criminalidade e as novas tecnologias da informação e comunicação". **Canal Ciências Criminais**. Jan. 2016. Disponível em: < https://canalcienciascriminais.com.br/criminalidade-e-as-novas-tecnologias-da-informacao-e-comunicacao/>. Acesso em: mar. 2018.

problemática, e divergências e possíveis soluções para o melhor aprofundamento e reflexão sobre o tema.

O motivo da escolha do tema é atribuído ao que se vê diariamente nos tribunais e nos âmagos dos lares de grande parte da população brasileira. A necessidade de enfrentamento correto dessa questão se faz extremamente necessária para que o Estado possa apaziguar o anseio da sociedade por uma tutela de todos os seus bens jurídicos.

No que concerne aos agentes que estão envolvidos pela temática, que têm a responsabilidade a obrigação de busca uma resolução para os conflitos, pode–se dizer que não se sabe se estão ou não atuando nesse sentido, e além disso, se estão sendo feitas de forma apropriada.

De outro modo, o próprio Estado se vê posto em uma situação de ameaça. Seu sistema Democrático de Direito vê um dos princípios basilares do ordenamento jurídico, o da legalidade, previsto nos artigos 1° do Código Penal e 5°, inciso XXXIX da Constituição da República Federativa do Brasil, posto em xeque.[3]

Isso se verifica no momento em que se pode chegar à conclusão de que as interpretações das Cortes jurídicas do país estão fazendo interpretação da lei penal a partir da analogia, ou até mesmo em interpretação analógica extensiva (que apesar de possível, não o é quando feita in malam partem).[4]

Para tal, o presente trabalho analisará, primeiramente o tema de forma geral, para depois aprofundar-se em uma (ou, pela conclusão, duas) conduta penalmente relevante, a descrita pelo crime de furto. Isso, quando praticado no ambiente cibernético, ou por dele.

Inicialmente será trazido o conceito de internet, com todas as suas peculiaridades, desde o seu conceito mais elementar, até seus possíveis desdobramentos para o futuro. Aqui, em adiantado, pode ser dito que é um complexo de diversas redes,

---

[3] SOUZA, Artur de Brito Gueiros; JAPIASSÚ, Carlos Eduardo Adriano. **Curso de Direito Penal**. v. 1. Campus Jurídico, 2012. p. 74.
[4] GRECO, Rogério. **Curso de Direito Penal:** Parte Geral. v. 1. 16. ed. Rio de Janeiro: Impetus, 2014. p. 45.

com objetivo final de permitir a troca de dados entre os usuários. (site que usei de fonte).[5]

Foi criada em um contexto de guerra- fria, com o objetivo de atender à vontade norte-americana de se igualar aos soviéticos na disputa pela supremacia tecnológica. Na época, não em criar uma rede de comunicações entre usuários do mundo inteiro, mas uma que permitisse o contato e transmissão de dados de uma unidade militar norte-americana para outra, acelerando o que antes era feito apenas por meios físicos.

Após o período de guerra supramencionado, a tecnologia vem em um crescente de ligar cada vez mais pessoas a partir do seu uso. O envio e recebimento de informações e dados se tornou essencial para a vida do cidadão comum.[6] Essa expansão da atividade humana possibilitou não só espaço para o desenvolvimento de atividades benéficas para a sociedade. Algumas são as que já ocorriam fora do ambiente virtual e eram combatidas pelo Estado.

Muitas são consideradas penalmente relevantes, tendo suas existências previstas nos tipos penais da legislação brasileira. Destaca-se, dentre elas, a de subtração de coisa alheia, que quando considerada "móvel", e sendo para si ou para outrem, encontra-se prevista no caput do artigo 155 do Código Penal.

Esse destaque se dá pela repercussão negativa que esse crime tem trazido à sociedade. Uma parte deste trabalho é destinada a mostrar os números, dados dos danos econômicos e sociais que são frutos da prática deste delito.

Tem sido decidido (e será mostrado e analisado) pelos Tribunais brasileiros que, quando praticado o ato de subtração de coisa alheia móvel por meio cibernético, enquadra-se na hipótese descrita pelo parágrafo 4°, inciso II do artigo 155 do Código Penal, sendo desclassificada a conduta de estelionato para ser a do furto qualificado por fraude.

---

[5] INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009. p. 171.

[6] CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 22.

No dia 17 do mês de junho deste ano, saiu, e foi também analisado pelo presente trabalho, a decisão sobre a conduta chamada de “furto bancário”, via internet. Este foi classificado, também, pelo STJ, como o descrito no inciso II, do parágrafo 4° do artigo 155, CP.[7]

Outra hipótese é quando o ato da subtração é praticado, mediante invasão de dispositivo informático, com o objetivo de se obter dados. Fica o debate se esse ato é realmente de subtração ou não, já que o bem não é retirado da esfera de proteção do indivíduo. É feita, na verdade, uma cópia do dado acessado.

Outro ponto é que tal conduta delitiva não é tipificada pelo artigo supramencionado, e sim pela lei 12.737/12, conhecida como lei Carolina Dieckmann, que alterou o Código Penal do Brasil para incluir (e modificar), dentre outros artigos, o que se refere ao “furto de dados: artigo 154-A.

A partir dessa apresentação, são feitas considerações à essa lei, mostrando pontos positivos e negativos, com construção e fundamentação de toda essa crítica. Aqui, desde já, pode ser dito que a lei, em sua cominação legal, previu a pena de detenção, de 3 meses a 1 ano, e multa. A contida no artigo 155, §4°, inciso II, em contrapartida, é de reclusão, de 2 a 8 anos, e multa.

Tudo isso, sempre trazendo à tona o princípio da reserva legal, prevista no art. 5°, inciso XXXIX da Constituição Federal e artigo 1° do Código Penal, segundo o qual, abre-se na doutrina uma discussão sobre a possibilidade ou não de tratar “dado” como coisa alheia móvel ou não.

O crime perpetrado por meio da internet, quando voltado para a obtenção de dados, se não fosse pela existência da lei 12.737/12, seria (ou deveria ser) atípico?

---

[7] BRASIL. Supremo Tribunal de Justiça. Conflito de Competência nº 145.576 - MA (2016/0055604-1). Suscitante: Juízo de Direito da 1ª Vara Criminal de Imperatriz - MA. Suscitado: Juízo de Direito da 1ª Vara Criminal de Bat. Relator: Ministro Joel Ilan Paciornik. Brasília, 20 de abril de 2016.

Para parte da doutrina, sim. Isso porque, respeitando-se o princípio da estrita legalidade, ou da reserva legal, a interpretação da lei penal não pode ser feita para pior (in malam partem) em relação ao aplicado ao acusado.[8]

Tal situação estaria acontecendo no momento em que for considerado "dados" como "coisa alheia móvel". Argumentam, este lado da doutrina que, assim como foi feito no §3° do artigo 155 do CP, no qual a energia elétrica foi equiparada a coisa alheia móvel, "dados" deveria ser considerado como tal, somente a partir de uma inclusão legislativa no texto legal.[9]

A outra parte defende que não. Trata-se mesmo de hipótese descrita no Caput do artigo supramencionado, e o bem jurídico tutelado é mesmo o patrimônio, e não, como alguns na doutrina alegam, outro, como o direito a "segurança informática".[10]

[8] MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018. p. 129.
[9] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. São Paulo: Saraiva, 2011. p. 16.
[10] BECK, Ulrich**. Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Editora 34, 2010. p. 383.

1 HISTÓRIA E EVOLUÇÃO DIGITAIS

1.1 HISTÓRIA DA INTERNET

A rede mundial de computadores, ou simplesmente internet, surgiu a partir do sucesso de um projeto da Advanced Reserch Projects Agency (ARPA), dos Estados Unidos, em setembro de 1969: a Arpanet. Esta não era mais do que um dos setores da ARPA, que havia sido criada com o objetivo de fazer frente ao grande avanço tecnológico da União Soviética, rival do governo americano, em um contexto de bipolarização mundial e Guerra Fria.

O estudo desenvolvido nesse setor era voltado para a criação de um mecanismo que permitisse aos usuários de computadores diferentes interagirem entre si. Isso foi feito a partir de uma tecnologia inovadora de transmissão de telecomunicações, a comutação por pacote. Com o desenvolvimento e aprimoramento desta rede de computadores, outras foram criadas e conectadas a essa, como a PRNET e a SATNET, formando um sistema de redes.

Para que estas redes se conectassem e pudessem interagir entre si, era necessário que fosse criado um padrão de protocolo de comunicação a ser seguido. Este foi criado a partir de um projeto, denominado TCP, feito com base em estudos encabeçados por Cerf, Gerard Lelann, e Robert Metcalfe, no ano de 1973.

Após cinco anos de desenvolvimento do projeto, em 1978, o TCP foi dividido em partes, numa das quais foi criado o protocolo intra- rede, o IP. Já no início da década de 90, a tecnologia da rede de computadores estava em domínio público, permitindo eu várias redes fossem criadas e se conectassem, distribuídas pelo mundo inteiro.

O ARPANET, apesar de não ter sido o único projeto que versasse sobre esse sistema, foi o pioneiro, tendo suas bases conservadas até a presente data, com funcionamento a partir de múltiplas camadas, sempre descentralizadas e com protocolos abertos.[11]

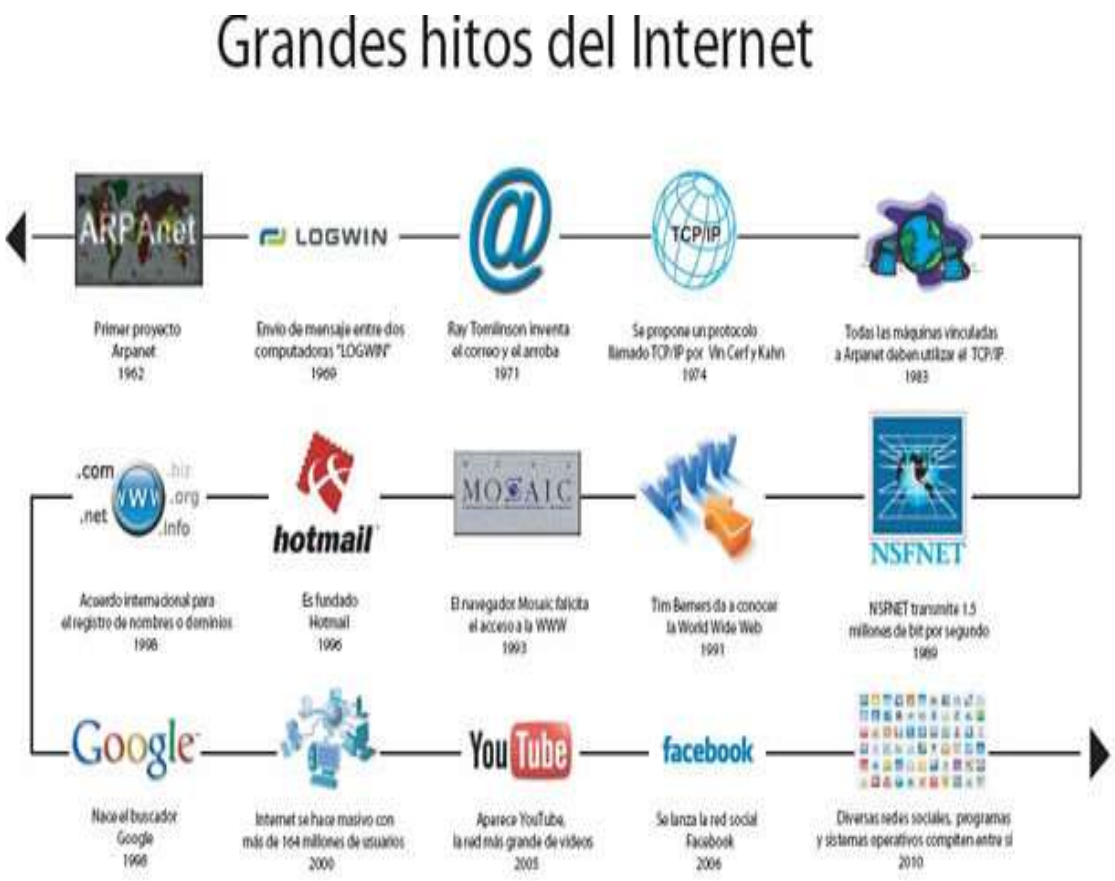
[11] CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003. p. 15.

Outros onze anos se passaram e, em Genebra, o *World Wide Web*, representado pela sigla *WWW*, foi criado, representando a rede mundial de computadores, aberta ao público mundial.[12] É por meio deste sistema que, até os dias atuais, é possível que haja interatividade, entre usuários de unidades de computação, para o envio de documentos que contêm sons, textos e imagens.

A internet pode ser conceituada como um complexo de diversas redes, com objetivo final de permitir a troca de dados entre os usuários. Esse complexo interativo só é possível a partir de uma padronização na forma como vai enviar e receber esses dados. Tal padrão foi obtido com a criação e utilização de protocolos. Um deles é o TCP, que essencialmente é o que permite a emissão e recepção dos dados, fazendo também uma organização deles. Outro deles é o IP, que estabelece um padrão entre redes próximas em uma determinada localidade, possibilitando que seja feito o ajuste do roteamento, que é o mecanismo pelo qual a conexão entre as redes tem uma rota definida. A partir do IP, então, também pode-se haver controle do envio dos dados, uma fiscalização.[13]

[12] INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009. p. 171
[13] Idem.

Imagem 1: "Grandes marcos da internet"



Fonte: Retirada do artigo de CHONG, Jorge. **Internet en las Organizaciones**, Los hitos, mas importantes de Internet. Disponível em: <https://jorchong.wordpress.com/2014/10/22/los-hitos-mas-importantes-de-internet/>. Acesso em: jun. 2018.

Alguns dados técnicos sobre o funcionamento dos mecanismos da internet são, aqui, interessantes de se tratar. Termos como HTML; HTTP; e WWW serão rapidamente explicados, após a explanação da história da criação desse ambiente no qual o tema (furto no meio cibernético) da presente obra ocorre.

Segundo Karen Gorthals[14], em uma de suas obras descreve tais termos como:

> HTML: Conjunto de códigos de marcação através dos quais são formatados os textos das páginas da WWW. Permite introduzir, formatação de texto,

[14] GOETHALS, Karen; AGUIAR, Antónia; ALMEIDA, Eugénia. **História da Internet**, 2000. f. Dissertação (mestrado) - Curso de Mestrado em Gestão da Informação, Faculdade de Engenharia da Universidade do Porto, Porto, 2000. s/p.

> incluir elementos multimídia (sons, imagens, sequências de vídeo, ...), bem como estabelecer hiperlinks entre diferentes documentos, ou entre zonas distintas de um mesmo documento - irás aprender como fazer isso mais para a frente neste curso -.
> HTTP: designa o protocolo usado para a transferência de páginas HTML na WWW.
> WWW: É uma rede virtual, dentro da internet constituída pelos servidores de documentos HTML, e pelos computadores clientes que acedem aos servidores, usando o protocolo HTTP.

O impacto da internet ocorreu em todos os campos da vida humana. Na economia, a partir de 1994, chegou ao número de milhões de usuários. Com isso, a publicidade, informações e prestações de serviços voltaram suas atenções para o meio. O comércio eletrônico tornou-se um novo propiciador do capitalismo moderno.

As suas implicações sociais foram de grande relevância também, gerando uma evolução cultural e econômica na sociedade. Os governos dos países passam a enxergar a necessidade de seus cidadãos terem a capacidade de lidar com a nova tecnologia. Há fomento para especialização e dinamização da produção dos mais diversos setores da sociedade.

Com tal importância dada a essa nova realidade, passa-se a buscar segurança nas transações, que são potencias alvos de delitos das mais variadas espécies. Já que as mensagens contendo dados e informações podem ser interceptadas (ou subtraídas), passa-se a fazer a encriptação dos dados.

Ainda segundo Karen Gorthals, a criptografia possui, além de um conceito, todo um mecanismo de funciomento específico:

> É uma forma de escrita codificada, onde o processo de codificação da mensagem se designa por cifragem e transforma a mensagem num criptograma.
> O processo de recuperação da mensagem original a partir do criptograma denomina-se decifragem.
> Os algoritmos de criptografia, também denominados por cifras, são funções matemáticas que fazem a cifragem e a decifragem, tendo em geral, dois componentes:
> O algoritmo de cifragem e o algoritmo de decifragem.
> Criptanálise é a ciência de quebrar criptogramas, ou seja, descobrir como fazer a decifragem de um criptograma, sem saber à partida como é que ele foi cifrado.

1.2 CENÁRIO DOS DANOS CAUSADOS NO MEIO CIBERNÉTICO

A nova realidade em que se depara a sociedade, trouxe consigo, além de todos os avanços e benefícios em geral, problemas graves, com repercussões ainda maiores, caso não sejam enfrentados.

Uma nova gama formas de perpetração de novos e antigos delitos está à mostra, podendo-se verificar os danos causados por eles, a partir de dados e estatísticas a seguir apresentados, vindos de manchetes e notícias, veiculadas pelos mais diversos meios de comunicação, tanto no Brasil, quanto no mundo.

No dia 17/06/2018, o Superior Tribunal de Justiça publicou dado estatístico sobre casos de julgamento dos crimes cibernéticos no Brasil. Estima-se que 62 milhões de pessoas são afetadas anualmente e há prejuízo de US$ 22 bilhões, de acordo com estudo divulgado no início de 2018 pela empresa de segurança virtual Symantec.[15]

Com o uso cada vez maior da rede mundial de computadores, espaços estão sendo abertos para a prática de novos delitos, ou até dos mesmos que já são tipificados. Agora, porém, por outros meios mais sofisticados e de maior dificuldade de solucionamneto por parte da polícia. O STJ vem trabalhando no sentido de trazer interpretações infraconstitucionais para os delitos cometidos no ambiente cibernético.[16]

Um relatório divulgado em fevereiro passado pela companhia holandesa de segurança digital Gemalto indica que mais de 1.500 vazamentos de dados por hackers em 2014 levaram ao comprometimento de mais de um bilhão de informações durante o ano — um aumento de 78% em comparação com as informações comprometidas em 2013.[17]

Já a Kaspersky Lab, uma das maiores empresas de segurança de TI do mundo, informa ter registrado o bloqueio de mais de 6,2 bilhões de ataques maliciosos em

---

[15] REVISTA CONSULTOR JURÍDICO. **"STJ divulga jurisprudência sobre conceitos de crimes pela internet"**. Disponível em: <https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet>. Acesso em: 20 jun. 2018.

[16] Idem.

[17] Idem.

computadores e dispositivos móveis por seus antivírus em 2014 — um bilhão a mais que em 2013.[18]

Por aqui, o país ainda carece de uma base de dados centralizada e oficial sobre ataques digitais, porém, levantamentos diversos mostram que vítimas como Pereira são cada vez mais numerosas. Informações do Centro de Estudos, Respostas e Tratamento de Segurança (Cert.br) indicam que, de 2013 para 2014, o número de notificações de ciberataques reportadas à entidade aumentou 197%: de 352.925 incidentes para 1.047.031, a maioria absoluta (44%) composta de tentativas de fraudes(outro).[19]

Dados trazidos em setembro de 2015, por uma seguradora alemã, revelam que o Brasil é o quarto país no ranking dos que sofrem mais prejuízos com os crimes cibernéticos. Essa seguradora, Allianz Global Corporate & Specialty (AGCS) mostrou, com base nesse levantamento, que a média anual dessas perdas é de 7,7 bilhões de dólares no Brasil. Nos Estados Unidos é de 108 bilhões; na china é de 60 bilhões, e na Alemanha é de 59 bilhões de dólares.[20]

A Allianz faz um alerta de que a tendência mundial é que os gastos, e, portanto, os custos dos riscos para cobrir danos com crimes cibernéticos, aumentem. Isso, devido à evolução da especialização e sofisticação dos criminosos da área, além do crescimento do número desses. Há um estudo da consultoria Pwc, de que 43 milhões de ataques foram reportados no ano de 2014 no mundo inteiro, que, distribuídos ao dia, gera o número alarmantes de 100.000 por dia.

Chris Fisher Hirs afirma que houve uma grande evolução na sofisticação dos ataques cibernéticos que, há 15 anos eram “rudimentares”. Além disso, continua dizendo que antes erma normalmente praticados apenas por hacktivistas (posteriormente explicados aqui na presente obra). O aumento das transações econômicas, causado pela

---

[18] MATSUURA, Sérgio; JANSEN, Thiago. **“Onda de crimes praticados por hackers cresceu 197% no Brasil em um ano”.** O Globo. Disponível em: <https://oglobo.globo.com/sociedade/tecnologia/onda-de-crimes-praticados-por-hackers-cresceu-197-no-brasil-em-um-ano-17197361#ixzz5JlOe8bth >. Acesso em: 12 jun. 2018.

[19] Idem.

[20] Idem.

globalização, e consequentemente, do fluxo de dinheiro, fez com que o ramo da criminalidade crescesse, trazendo um novo perfil de hacker, ou cracker, na verdade.[21]

As apólices de seguros, prontamente, têm sido modificadas, cada vez mais, para atender aos anseios dos compradores, que necessitam cada vez mais, de uma maior abrangência na cobertura de seus produtos e serviços, alvos potenciais dos praticantes do "ciberdelitos". A cultura do asseguramento desses bens ainda é restrito a alguns comerciantes, daí e apontado umas das causas dos números dos danos causados por esses crimes aos usuários.

Esse costume se concentra principalmente nos EUA, com 90% dos prêmios feitos no país, na data do estado. A tendência, no entanto, é do crescimento dessas no mundo inteiro, diminuindo essa concentração da proporção dos seguros. E um mercado com valor estimado de 2 bilhões de dólares, representando expressivo valor. [22]

As estatísticas de crescimento mostram que, apesar de alto, esse valor de mercados das seguradoras aumentará em 10 vezes nos próximos anos, chegando a marca surpreendente de 20 bilhões de dólares.[23]

Tudo isso porque, como a lógica indica, os crimes e seus danos patrimoniais crescerão, também, nesta mesma proporção. A média de prejuízo para uma empresa após um único ataque desse tipo é de 3,8 milhões de dólares, segundo a seguradora. A matéria traz o exemplo da loja Target, que em 2014 teve um prejuízo de mais de 100 milhões de dólares por causa dessas ações.[24]

A proteção buscada é baixa, por parte dos comerciantes, em relação ao tamanho dos riscos existentes. As seguradoras, de outra forma, também não oferecem ainda, de maneira apropriada, a cobertura correta para aqueles que procuram fazê-la. O maior valor oferecido no mercado gira em torno de 500 milhões de dólares, o que não chega

---

[21] AMARAL, Rodrigo. **"Brasil é quarto em ranking de danos causados por cibercrime"**. Risco Brasil Seguro (site). Disponível em: <http://riscosegurobrasil.com/materia/brasil-e-quarto-em-ranking-de-danos-causados-por-cibercrime/>. Acesso em: 18 mai. 2018.
[22] Idem.
[23] Idem,
[24] Idem.

perto de ser o ideal para cobrir o fluxo de movimentação das grandes companhias que praticam o e-commerce.

Quanto à privacidade, pode ser dito que está necessita de um aumento do rigor das leis que versam sobre o assunto. Esta é, segundo a Allianz, a tendência mundial, que vê os dados pessoais de usuários como bens ainda vulneráveis nesse meio cibernético.

Em países como Estados Unidos, Austrália, Cingapura e Hong Kong, regras mais estritas já são uma realidade, enquanto que a União Europeia está caminhando rumo a uma legislação comum para todos os países-membros.

Tal informação demonstra que as multas e demais sanções estão aumentando em termos de expressividade para aquelas empresas que não conseguem proteger dos hackers os dados dos usuários que confiaram suas informações a elas.

Apesar de o tema do trabalho estar voltado para o crime de maior relevância, em termos de danos financeiros, o furto, outros crimes também são praticados pelo meio cibernético, a se destacar a extorsão e o roubo de propriedade intelectual, mostra o estudo.

Outra informação é que nem sempre os ataques são contabilizados, por se tratarem de propaganda negativa para as empresas que foram alvos desses ataques. Esses ainda são repentinos e atingem muitas das empresas porque os próprios operadores da computação não compreenderam ainda as dimensões dos riscos existentes, e quais devem ser as precificações dos custos para determinadas prestações de serviço de segurança. Hackers, por exemplo, se aproveitam dos momentos de mudanças nos sistemas de informação para atacar.

A conectividade, que caracteriza de forma mais elementar o conceito de internet, (colocar algum conceito de alguém) é também um fator de risco para o aumento exponencial dos danos causados pelos hackers, que de sistema informático, consegue atacar outros a partir dos dados contidos naquele, e assim sucessivamente. Em 2020 a expectativa é de que haja 1 trilhão de dispositivos informáticos, desde computadores

tradicionais, até os dispositivos móveis, como celulares e tablets. Todos esses, sujeitos a ataques desse tipo.[25]

A forma como os crimes são praticados também são diferentes dos meios usuais quando ocorre por meio da internet. Para acessar dados e informações dos usuários e romper barreiras e dispositivos de segurança, usa-se mecanismos com conceitos técnicos sofisticados, que são, porém, atualmente, comuns. Um dos mais conhecidos é o "pishing".

Esse nome vem do termo "fishing", que significa pescar, em inglês. O método é parecido com o da pesca: uma isca é lançada para atrair os usuários para um site. Após clicar nele e ter o acesso, este usuário já terá caído no golpe, permitindo que malwares entrem em seu dispositivo informático e acesse seus dados, sem seu consentimento.

Segundo João Kurtz, esse crime tem como principal alvo usuários comuns, e propaga-se rapidamente, já que encontra em plataformas de compartilhamento de dados o ambiente ideal para a prática.[26]

> A forma de transmissão mais comum de um ataque de phishing é através de redes sociais, especialmente o Facebook, que é alvo de vários tipos de golpes devido a sua popularidade. Uma conta infectada é usada para publicar um link em seu mural prometendo um conteúdo que tem grandes chances de chamar a atenção de outras pessoas.
>
> É comum que estes links façam referências a curiosidades ou a eventos e feriados próximos, como o Natal e a Black Friday. Ao clicar nele, o internauta é enviado a um site que pede a instalação de um aplicativo ou extensão extra para reproduzir o conteúdo, ou tenta reproduzir ele mesmo o arquivo infectado. Ao fazer isso, a conta da pessoa em uma rede social também é infectada, sendo usada para espalhar o golpe.[27]

---

[25] AMARAL, Rodrigo. **"Brasil é quarto em ranking de danos causados por cibercrime"**. Risco Brasil Seguro (site). Disponível em: <http://riscosegurobrasil.com/materia/brasil-e-quarto-em-ranking-de-danos-causados-por-cibercrime/>. Acesso em: 18 mai. 2018.

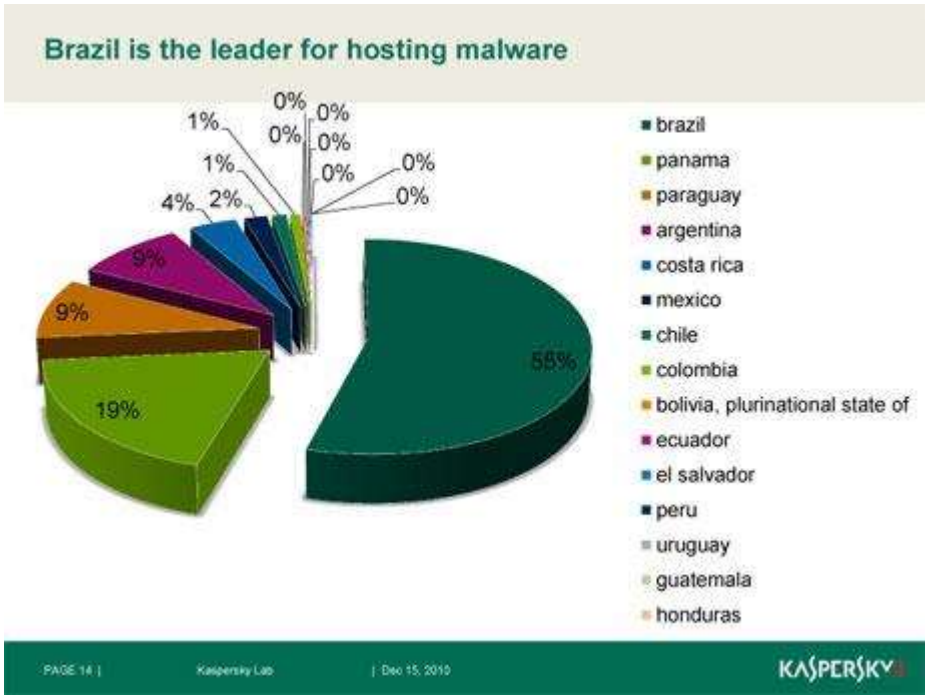
[26] KURTZ, João. **"O que é phishing?"**. Techtudo (site). Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-phishing-e-malware.html>. Acesso em: jun. 2018.

[27] Idem.

Imagem 2: Perda de tempo e dinheiro para o crime cibernético.

Fonte: Retirada do artigo de SILVA, Rafael. **"Gasto com crimes virtuais no Brasil em 2010 foi de US$ 15 bilhões, diz Symantec"**. Disponível em: <https://tecnoblog.net/77490/symatec-crimes-virtuais-2011/>. Acesso em: jun. 2018.

Imagem 3: “O Brasil é o líder de hospedagem de malware”



Fonte: Retirada da página SATTOTAL. **“61% dos PCs brasileiros foram infectados com malwares de roubos de dados bancários em 2010”.** Disponível em: <http://sattotal.blogspot.com/2010_12_12_archive.html>. Acesso em: jun. 2018.

2 O MECANISMO DO CRIME CIBERNÉTICO

2.1 DIREITO À PRIVACIDADE

A temática da proteção e tutela do Estado aos indivíduos, em relação aos direitos à privacidade, tem sido cada vez mais analisados no meio acadêmico e jurídico em geral. Isso se deve, em grande parte, à difusão exponencial e relativamente recente das tecnologias da computação, sobretudo com a maior gama de possibilidades de interação entre as pessoas.

Marcelo Crespo traz a temática à tona, alertando sobre o surgimento de sites violadores dos direitos ligados à privacidade e à intimidade, em trecho inicial de artigo:

> Está se tornando comum o surgimento de sites que divulgam dados pessoais dos internautas, tais como o CPF, endereço, CEP e até mesmo nomes de possíveis vizinhos. São exemplos o www.nomesbrasil.com, (...). A utilização destes sites é bastante fácil (algumas consultas são cobradas), bastando digitar um nome e verificar as informações constantes da base de dados online. Por causa disso, a indignação pública sobre a publicidade da divulgação sem autorização também tem aumentado e as discussões tem sido mais intensa, sem, todavia, haver consenso sobre a (i)licitude desta prática.[28]

Segundo José Afonso da Silva, o conceito de privacidade pode ser definido como: *"o conjunto de informações acerca do indivíduo que ele pode decidir manter sob o seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem isso pode ser legalmente sujeito".*[29]

Já para Celso Bastos privacidade é:

> "faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada

[28] CRESPO, Marcelo. **"Sobre os sites que divulgam dados pessoais: uma análise sob a perspectiva criminal"**. Disponível em: <https://canalcienciascriminais.com.br/sobre-os-sites-que-divulgam-dados-pessoais-uma-analise-sob-a-perspectiva-criminal/>. Acesso em: jun. 2018.

[29] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 11. ed. São Paulo: Malheiros, 1996. p. 818.

> um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".[30]

O avanço trazido à humanidade como um todo, pelo advento da internet, é incomparável aos danos causados por ela. Com a maior conectividade entre os usuários do mundo inteiro, trocas se tornaram mais frequentes, e fronteiras agora são permeáveis à informação.

No entanto, tais danos devem ser levados em consideração. Junto às novas possibilidades de trocas, a prática de crimes também encontrou novos caminhos. Alguns passaram a ser perpetrados por meio dela, e outros surgiram a partir dessa nova etapa em que a sociedade se encontra. Os chamados cibercrimes surgem, violando direitos diversos (dentre eles, o à privacidade).

2.2 JURISDIÇÃO DIGITAL

Jurisdição, segundo Chiovenda, é, essencialmente, a troca da aplicação de uma justiça feita por particulares que tenham sofrido o dano, pela atuação do Estado nesse sentido. Isso é feito a partir do conteúdo das leis: *"a jurisdição consiste na atuação da lei mediante a substituição da atividade alheia pela atividade de órgãos públicos, afirmando a existência de uma vontade da lei e colocando-a, posteriormente, em prática".*[31]

O Estado, que não tem interesse no conflito entre as partes, atuando como um mediador e juiz, buscando a efetividade de suas ações, seja por meio coercitivo ou não. Essa jurisdição pode ser voluntária ou contenciosa.

Enquanto na contenciosa o Estado tem um papel ativo em todas as partes do processo, decidindo sobre a causa controvertida entre as partes, tanto sobre o mérito da

---

[30] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. v. 2. São Paulo: Saraiva, 1989. p. 295.

[31] CHIOVENDA, Giuseppe; ATHENIENSE, Alexandre. **A Jurisdição no Ciberespaço**. Revista Jurídica do CEJ (Centro de Estudos Judiciários). Brasília: Conselho da Justiça Federal, ano 7, nº 20, p. 75, 2003.

causa, quanto sobre a medida a ser tomada para a reparação do dano, na voluntária tem o papel, em suma, de homologar o decidido e acordado por elas.[32]

A lei, para exercer seu papel, tem a necessidade de ter definidos os locais onde o poder judiciário tem competência. Adota-se, então, critérios para tal, norteados por princípios do direito penal, para tal

O grande objetivo é impedir a existência de lugares onde não há jurisdição de qualquer Estado. Nas palavras do Professor Japiassú, paraísos penais, por conta de um conflito negativo de jurisdições:

> "Para que a lei cumpra as funções é necessário que seja determinado em que locais poderá o judiciário brasileiro exercer sua competência. Sobre o assunto, o código Penal estabelece que a lei possa alcançar fatos cuja persecução penal seja do interesse do Estado Brasileiro. Por intermédio de tais critérios pretende-se basicamente evitar que ocorram lacunas de impunidade a respeito de ilícitos que atinjam bens jurídicos tutelados(...) generalidade dos Estados adota (...) espécie de malha de leis penais, circunstância essa que redunda quase impossibilidade de "conflitos negativos de jurisdições", ou seja, o surgimento de "paraísos penais"

Um princípio, adotado pela legislação brasileira como norteador da incidência da jurisdição é o da territorialidade, segundo o qual a lei penal deve ser aplicada onde o Estado exerce a sua soberania, independendo da nacionalidade ou do agente ou da vítima.[33][34]

---

[32] COSTA JÚNIOR, Dijosete Veríssimo da. **Jurisdição contenciosa e jurisdição voluntária**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 13, 18 maio 1997. Disponível em: <https://jus.com.br/artigos/776>. Acesso em: jun. 2018.

[33] SOUZA, Artur de Brito Gueiros; JAPIASSÚ, Carlos Eduardo Adriano. **Curso de Direito Penal**. v. 1. Campus Jurídico, 2012. p. 100.

[34] Artigo 5º do Código Penal: "Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional. (Redação dada pela Lei nº 7.209, de 1984)

§ 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar. (Redação dada pela Lei nº 7.209, de 1984)

§ 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em voo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil. (Redação dada pela Lei nº 7.209, de 1984)"

Algumas teorias que tratam do assunto, no entanto, também devem ser levadas em consideração. Segundo a da atividade, é a ação ou omissão que define o crime, não havendo importância quanto ao local da ocorrência do resultado. Pela do resultado, tem-se o contrário: o local do resultado é o que define o local do crime. Por último, segundo a teoria da ubiquidade, as duas opções e fatores das anteriores devem ser levados em consideração para a determinação do local do crime e, consequentemente, a aplicação da jurisdição brasileira. O local do crime, por tanto, pode ser definido, segundo essa, tanto pelo local onde houve a ação ou omissão, quanto pelo local onde produziu ou deveria produzir seu resultado.[35]

A nossa legislação adotou, por meio do Código Penal Brasileiro, esta teoria, como se extrai do contido no seu artigo 6°: *"Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado."*

Recentemente, STJ decidiu sobre a competência do juízo quando da prática de um crime praticado por meio da internet. No caso, apreciado no CC 145576 MA 2016/0055604-1, foi o crime de "furto bancário", tipificado pelo Código Penal em seu artigo 155, parágrafo 4°, inciso II, tratando-se de furto qualificado (por fraude).

Na decisão, estabeleceu a Corte que o local por a vítima sofreu o ataque é o determinante para a competência do juízo, conforme leitura de parte do acordão:

> O presente conflito de competência deve ser conhecido, por se tratar de incidente instaurado entre juízos vinculados a Tribunais distintos, nos termos do art. 105, inciso I, alínea "d", da Constituição Federal. Com razão o Juízo suscitante. O caso dos autos trata-se de hipótese em que ocorreu transferência eletrônica fraudulenta, via internet, sem consentimento da vítima, de contas situadas em agência do Banco Santander de Barueri/SP para conta corrente em agência do referido banco em Imperatriz/MA. O fato investigado acima não configura crime de estelionato, no qual a consumação se dá com a obtenção da vantagem ilícita, mas sim o crime tipificado no art. 155, § 4º, II, do Código Penal, cuja consumação ocorre com a retirada do bem da esfera de disponibilidade da vítima. Esta egrégia Terceira Seção firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal (...) Nesse diapasão, o delito em

[35] GRECO, Rogério. **Curso de Direito Penal:** Parte Geral. v. 1. 16. ed. Rio de Janeiro: Impetus, 2014. p. 131.

> questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, sendo, portanto, competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, nos termos do art. 70 do CPP. Ante o exposto, voto no sentido de conhecer do presente conflito de competência para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP , o suscitado.[36]

2.3 O AGENTE DO CRIME

A internet é, ainda hoje, um ambiente relativamente inóspito. Diante de tamanha liberdade de produção e acesso a conteúdo por quem quer que seja o usuário, indivíduos perceberam ser um local propício para práticas delitivas. Além do pouco regramento, há a facilidade da desnecessidade do deslocamento físico para a ação do criminoso e o anonimato das ações, feito por meio de técnicas que burlam os precários meios de fiscalização no meio cibernético.

O perfil usual deste indivíduo é o do jovem, que é encontra na faixa de idade entra 16 e 32 anos, sexo masculino, branco, com inteligência acima da média, e que busca um auto superação em termos de conhecimento no ramo da computação. Desconhece o risco de implicação legal dos seus atos, diante da confiança de que não será pego, já que confia no anonimato proporcionado pela internet.[37]

Aqui, o agente dos delitos perpetrados por meios digitais, não será necessariamente o chamado hacker. Isso porque não há verdadeiro consenso sobre essa nomenclatura. Abaixo, como logo será, conceitua-se hacker não como o criminoso que prática delitos por meio da internet, como conhecidamente é denominado.

A “cultura-hacker” se iniciou entre as décadas de 1960 e 1970, a partir de um movimento intelectual, no qual se buscava a busca daquilo que não era conhecido pelo público em geral, referente à nova tecnologia que surgia: a internet.

---

[36] BRASIL. Supremo Tribunal de Justiça. Conflito de Competência nº 145.576 - MA (2016/0055604-1). Suscitante: Juízo de Direito da 1ª Vara Criminal de Imperatriz - MA. Suscitado: Juízo de Direito da 1ª Vara Criminal de Bat. Relator: Ministro Joel Ilan Paciornik. Brasília, 20 de abril de 2016.

[37] SILVA, Mauro Marcelo de Lima. Crimes de informática. 15. ed. São Paulo: Saraiva, 1997. p.147.

Vários grupos se formaram em diferentes e bem-conceituadas faculdades do mundo inteiro, formando verdadeiras comunidades de hackers. Com a conclusão do programa (já explanado no início da presente obra) ARPANET, houve a possibilidade de conexão entre esses grupos, por meio da internet, surgindo o ambiente, também, propício para os surgimentos dos "criminosos da computação".[38]

Há, no meio informático, vários tipos de práticas criminosos. Muitas delas são praticadas por pessoas sem qualquer qualidade específica ou conhecimento técnico. Outras, porém, por suas áreas de atuação e motivo que os move, podem ser bem definidas. Aqui, agora, serão tratados algumas dessas pessoas.

O primeiro a ser dito é o chamado "cracker". Este é, pelos provedores e sistemas de segurança, aquele que gera mais danos aos dispositivos ligados à rede mundial e computadores. Suas maiores motivações são vantagens econômicas e o reconhecimento de atuantes da área do tamanho de suas habilidades. Isso é atingido por meio da invasão de sistemas com avançados mecanismos de segurança, mas que, ainda assim, não são capazes de detê-los.[39]

O próximo a ser tratado é o mais conhecido, o hacker. Seu termo veio do inglês "to hack", que pode ser traduzido para o português como a expressão "bisbilhotar". Apesar o conhecimento geral o tratar como sendo aquele que invade dispositivos informáticos de forma ilegal, como foi supramencionado, este é o cracker. O hacker é, na verdade, um especialista em informática, que atua no sentido de descobrir defeitos nos mecanismos de segurança para dispositivos informáticos.

Após a descoberta, entram em contato com os operadores desses sistemas. É a pessoa que detém, como objeto do seu trabalho, a investigação da integridade e da segurança de um sistema de computação. Não prejudica ou destrói qualquer coisa.[40]

---

[38] CRESPO, Marcelo Xavier de Freitas. **"As diversas terminologias do universo hacker"**. Canal Ciências Criminais. Set. 2015. Disponível em: <https://canalcienciascriminais.com.br/as-diversas-terminologias-do-universo-hacker/>. Acesso em: 10 jun. 2018.

[39] Idem.

[40] PLANTULLO, Vicente Lentini. **Estelionato Eletrônico**. Curitiba: Juruá, 2003. p. 79.

Há também classificações que colocam o termo hacker como uma nomenclatura geral, abarcando tipos de criminosos específicos, aí sim divididos. Alguns deles precisam de conhecimentos técnicos específicos, e outros não, o que não impede que sejam classificados como criminosos cibernéticos.[41]

Há, de acordo com essa forma de caracterização, o 'cracker de servidores". Esse é o hacker que atua invadindo dispositivos informáticos ligados em rede. Outro é o "cracker de programas". São hackers que conseguem destruir programas de proteção de sistemas de computação. Softwares de proteção são seus alvos.

Um terceiro, terminando por aqui a lista dos que necessitam de conhecimentos técnicos para suas atividades, é o "Phreaker", que é um atuante na área da telefonia móvel ou fixa. Sua nomenclatura vem dos termos "phone" e "freak", que são "telefone" e "aberração", respectivamente. Suas principais formas de atuação nesse ramo são as de burlar o sistema de cobrança por ligações, locais ou interurbanas (o que perdeu grande relevância nos dias atuais, diante dos avanços nas comunicações e barateamento dos preços desses serviços); reprogramação de centrais telefônicas; e colocação, por meio de invasão, de escutas telefônicas não-autorizadas.

Os 3 últimos, como dito acima, não necessitam de conhecimentos técnicos. São eles: o "desenvolvedor de vírus, worms e trojans", que é um programador que cria pequenos softwares com o objetivo de causar danos aos usuários da rede de computadores; o "pirata", o hacker que atua na clonagem de programas, fazendo, principalmente, fraudes; e os "distribuidores de warez", que são donos de sites ou webmasters que permitem o acesso de usuários a conteúdos, em suas páginas, sem a autorização de qualquer tipo de quem tem os direitos autorais sobre aqueles conteúdos.[42]

---

[41] SILVA, Mauro Marcelo de Lima. **Os crimes digitais hoje**, 2000. Revista do Consultor Jurídico (online). Disponível em: <http://www.conjur.com.br/2000-set-02/policia_revela_perfil_criminoso_internet>. Acesso em: mai. 2018.

[42] VIANNA, Túlio Lima. **Do rastreamento eletrônico como alternativa à pena de prisão.** *In*: Revista da Ordem dos Advogados (A. 68, t. 2-3, set /dez. 2008). p. 901-914.

Há também os “SPAMMERS”, que fazem o envio descontrolado de mensagens que não foram requisitadas, e podem estar trazendo vírus consigo (são chamadas de spam). O termo vem também do inglês “spiced ham”, que é uma marca de presunto americana. Além disso, atuam captando endereços de e-mails e fazendo a venda desses. Uma das formas pelas quais conseguem fazer isso, é por meio de programas instalados em “correntes”, que são disseminadas pelos próprios usuários.[43]

Outro tipo de hacker é o “DEFACER”. São os “vândalos “de páginas na internet. Invadem, rompendo sistemas de segurança, dispositivos informáticos, obtendo acesso aos seus conteúdos. Depois de danificá-los, alteram o conteúdo da página, colocando um outro. Fazem isso, muitas vezes, com intuitos políticos, e o fazem a partir de várias brechas na segurança, como furto de senha do acesso para o site.[44]

Existem também os LAMMERS. São os crackers que ainda não possuem muito conhecimento. Fazem a mesma prática dos crakers, porém com menos potencial de danificação dos sistemas informáticos.

Seguindo a listagem dos hackers, os WANNABES são um tipo deles. Possuem esse nome porque aspiram ser especialistas. Sua diferença é que o WANNABE, diferentemente do LAMMER, reconhece sua posição de baixo conhecimento. LAMMER chega a ser um termo pejorativo para esse tipo de hacker.[45]

Há, ainda, os hacktivistas, que são crackers movidos por posicionamentos políticos, sociais e ideológicos.[46]

Todos esses hackers possuem uma característica em comum: normalmente têm como alvo bancos de dados. Esse é o criminoso que prática, com habitualidade, o crime

---

[43] CRESPO, Marcelo Xavier de Freitas. **“As diversas terminologias do universo hacker”**. Canal Ciências Criminais. Set. 2015. Disponível em: <https://canalcienciascriminais.com.br/as-diversas-terminologias-do-universo-hacker/>. Acesso em: 10 jun. 2018.

[44] Idem.

[45] Idem.

[46] BARROS, Laura. **O Hacktivismo no Desenvolvimento da Internet.** Anonymous Brasil (site). Disponível em: <http://www.anonymousbrasil.com/coluna/o-hacktivismo-no-desenvolvimento-da-internet/>. Acesso em: abr. 2018.

do “furto de dados”, tratado aqui no presente trabalho, daí a sua importância em conceitua-lo.

Esse dado é de um levantamento sobre os hackers que causaram mais danos na história recente da humanidade. Dentre eles estão os que são movidos pela vontade de ganhar dinheiro, e outros por inclinações políticas.

São conhecidos como “Black Hats”. Eles praticam o chamado terrorismo eletrônico. Roubam, principalmente, informações pessoais, arquivos confidenciais, e expõem a vida intima de celebridades. O governo americano, no ano de 2015, criou um grupo especializado que terá a única missão de capturar esses indivíduos. Da listagem que foi feita, aqui ficam algumas informações sobre alguns deles:

Albert Gonzalez fundador do Shadowcrew.com. Formou uma comunidade com 4 mil pessoas. Os membros tinham a oportunidade de cometer diversos delitos, facilitados por sua atividade. Algumas delas eram de comprar: números de contas correntes e passaportes, carteiras de motorista, números de seguro social, cartões de crédito, certidões de nascimento e carteiras de plano de saúde.

Aproximadamente 170 milhões de cartões de crédito e débito foram vendidos no site. Gonzalez com o dinheiro e fama que tinha. Pagava hospedagem em hotéis de luxo e fazia festas que custavam milhares de dólares. Foi imputado pela prática, quando pego, de diversos crimes, dentre eles o de falsidade ideológica e, depois de ter sido pego com 15 cartões bancários falsos em Nova Jérsei, tentou evitar ser preso dando nome de outros 19 membros da ShadowCrew. Ao retornar para Miami, invadiu o sistema de uma rede de lojas e roubou 45 milhões de cartões de crédito no decorrer de 18 meses. Foi preso em 2008 e irá ficar na cadeia até 2025.

O segundo da lista é Jonathan “c0mrad” James, que aos 15 anos de idade invadiu o sistema de segurança da NASA e do Departamento de Defesa americano. Obteve, por meio dessas invasões, softwares que valiam 1,7 milhão de dólares. Outra façanha de james teria sido interceptar o código da Estação Espacial Internacional, o que fez com que a NASA tivesse que desligar seu sistema de computação por 3 semanas, causando

prejuízos ao governo norte americano. No ano de 2008 se matou, por ter medo de ser preso pela suposta prática de um outro crime.

Outro nome da lista é o de Kevin Poulsen. Ele ficou famoso por ter sido o primeiro americano a ser banido da internet. Na década de 90, Poulsen invadia linhas telefônicas (como explicado anteriormente, tratava-se se de um "Phreaker"). Outra ação que o fez ficar conhecido foi a de ter conseguido entrar no sistema de rádio e ser o 102° ouvinte a ligar para uma rádio, que iria dar um Porshe para quem ligasse justamente nessa colocação. Atualmente escreve para uma revista de computação.[47]

Mais um exemplo de que tais práticas devem ser combatidas, aqui fica registrada a ação de um grupo que consta na lista da matéria anterior, desta vez, atundo no brasil, em data próxima da feitura deste presente trabalho de conclusão de curso.

O grupo de hackers autodenominados "Anonymous", viu um desmembramento de seu grupo no Brasil atuar em um vazamento de dados ligados ao presidente da República Michel Temer. Na ocasião, com a alteração de sites e páginas do governo, declararam apoio à greve dos caminhoneiros e se opuseram às medidas tomadas pelo presidente na tentativa de resolução do conflito, destacadamente, a de ter ordenado que as forças armadas desbloqueassem as rodovias.

Além disso, publicaram dados pessoais do presidente no site Ghostbin. Dados de funcionários públicos foram vazados e sites foram invadidos e modificados, deixando expostos em suas páginas, apoio à greve.[48]

Imagem 4: Membros do Grupo Anonymous.

[47] GARCIA, Gabriel. **"Os 15 hackers que fizeram os maiores estragos da história".** Revista Exame (online). Disponível em: <https://exame.abril.com.br/tecnologia/os-15-hackers-mais-perigosos-de-todos-os-tempos/>. Acesso em: 05 mai. 2018.

[48] AGRELA, Lucas. **"Grupo Anonymous ataca Temer e apoia greve dos caminhoneiros".** Revista Exame (online). Disponível em: < https://exame.abril.com.br/tecnologia/grupo-anonymous-ataca-temer-e-apoia-greve-dos-caminhoneiros/>. Acesso em: 10 jun. 2018.

Fonte: Retirada do artigo de GARCIA, Gabriel. **“Os 15 hackers que fizeram os maiores estragos da história”.** Revista Exame (online). Disponível em: <https://exame.abril.com.br/tecnologia/os-15-hackers-mais-perigosos-de-todos-os-tempos/>. Acesso em: 05 mai. 2018.

3 CRIME DE FURTO E A LEGALIDADE

3.1 FURTO

O crime de furto, previsto no artigo 155 do Código Penal brasileiro[49], possui características próprias e nuances, que aqui serão analisadas antes de se adentrar para o ato de mesmo nome quando praticado por meio da rede mundial de computadores.

Há, inicialmente, uma discussão elementar, quanto ao objeto em si alvo da tutela penal desse tipo penal. Nelson Hungria defende que esse é a propriedade. Noronha apoia que esse objeto, além da propriedade, também abarca a posse. Já para Heleno Fragoso, o objeto chega a ser mais extenso, devendo-se proteção para a posse, a propriedade, e também para a detenção legítima de coisa móvel.[50]

Quanto aos sujeitos do crime, pode se dizer que qualquer pessoa pode ser sujeita ativo, já que não é exigida qualquer qualidade especial para o agente, salvo o proprietário do bem, que estaria praticando, nessa situação, exercício arbitrário das próprias razões.[51]

O que se pode dizer, aqui, sobre a conduta, é que o apoderamento, por parte do agente, para si ou para outra pessoa, de coisa alheia móvel, retirando o bem da vítima, e consequentemente, diminuindo o seu patrimônio.[52]

---

[49] Artigo 155 do Código Penal: "**Furto**. Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
Pena - reclusão, de um a quatro anos, e multa.
§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico."

[50] CUNHA, Rogerio Sanches. **Manual de Direito Penal:** Parte Especial. 9. ed. Salvador: Editora Juspodivm, 2017. p. 269.

[51] Artigos 345 e 346 do Código Penal: "Exercício arbitrário das próprias razões. Art. 345 - Fazer justiça pelas próprias mãos, para satisfazer pretensão, embora legítima, salvo quando a lei o permite:
Pena - detenção, de quinze dias a um mês, ou multa, além da pena correspondente à violência.
Parágrafo único - Se não há emprego de violência, somente se procede mediante queixa.
Art. 346 - Tirar, suprimir, destruir ou danificar coisa própria, que se acha em poder de terceiro por determinação judicial ou convenção:
Pena - detenção, de seis meses a dois anos, e multa."

[52] CUNHA, Rogerio Sanches. **Manual de Direito Penal:** Parte Especial. 9. ed. Salvador: Editora Juspodivm, 2017. p. 271.

Segundo Rogério Sanches, o objeto material do crime deve ser, além de coisa alheia móvel, algo economicamente apreciável. Isso, apesar de saber que parte da posição doutrinaria em geral é no sentido de que não somente bens com tais características estão abarcados no objeto do tipo penal, mas também aqueles que a vítima tem interesse moral ou sentimental:

> "Da análise do tipo em estudo, fica claro que o objeto material do crime deve ser *coisa alheia móvel,* economicamente apreciável. O interesse apena moral ou sentimental da coisa, desde que relevantes, segundo alguns, também configura o crime, pois não deixa de integrar o patrimônio de alguém"

O contraponto é feito por outra parte da doutrina, no qual alega-se que objeto sem qualquer valor econômico não merece a tutela jurisdicional. Exemplo disse seria a coisa puramente de estimação. Caso esse objeto seja subtraído, a dor moral sentida pela vítima deve ser reparada na esfera civil, e não na penal.

Sobre a voluntariedade, pode ser dito que é a vontade consciente de obter coisa alheia. Deve, o agente, ter a intenção de ficar definitivamente com a coisa, sem devolvê-la à vítima. Quando for feita subtração com o único objetivo de usar a coisa e depois devolvê-la, sem qualquer dano a esse bem, trata-se de furto de uso, que é atípico.

Tratando agora da consumação e tentativa, aqui serão tratadas quatro correntes sobre o que define o momento da consumação: a *amotio,* segundo a qual a consumação se dá quando a coisa subtraída fica sob o poder do agente, não dependendo de qualquer outro fator, como posse mansa e pacífica, quando subtrai a o bem ; a *concrectatio*, que dispõe no sentido de que o crime de furto se consuma quando pelo mero contato entre o agente do crime e a coisa alheia móvel, sem a necessidade de deslocamento da coisa ; a *ablatio,* que traz o momento da consumação como aquele em que o agente, tendo se apoderado da coisa alheia móvel, consegue desloca-la para outro lugar que não o do local da subtração; e a *ilatio,* em que, para a ocorrência consumação, além do ato de subtrair a coisa de outrem, deve o agente ter conseguido fazer com que o bem esteja a salvo. [53]

[53] CUNHA, Rogerio Sanches. **Manual de Direito Penal:** Parte Especial. 9. ed. Salvador: Editora Juspodivm, 2017. p. 271.

O ordenamento jurídico pátrio, por meio de jurisprudência das principais Cortes do país, acabou por adotar a corrente do *amotio,* sendo considerado, então, consumado o crime de furto quando o proprietário do bem perde o contato, ou a opção de fazê-lo, com o bem móvel, independendo se isso se deu por causa da mudança de lugar deste pelo agente, seja por ele o destruiu ou deixou a salvo. É, em suma, a perda da possibilidade do proprietário de dispor sobre a coisa. [54]

Em rápidas linhas, agora, para esgotar a principais tratativas do crime de em espécie preconizado no artigo 155 do Código Penal[55], serão tratadas as hipóteses de tentativa; as qualificadoras; e majorante de pena.

Quanto à tentativa, pode-se dizer que está é admissível. Está caracteriza-se quando o agente, por circunstâncias alheias a sua vontade, não consegue o resultado desejado. No caso do furto, obter a posse da coisa, mesmo que por curto espaço de tempo.[56]

Há o caso da chamada tentativa inidônea, ou crime impossível, em uma discussão sobre o crime quando praticado pelo agente quando monitorado por sistema eletrônico de vigilância. Esta foi resolvida a partir da súmula 567 do STJ:

> Sistema de vigilância realizado por monitoramento eletrônico ou por existência de segurança no interior de estabelecimento comercial, por si só, não torna impossível a configuração do crime de furto.

Há também precedente do STF, a partir do HC 117.083/14 versando sobre o assunto: *"[t]ese de crime impossível. Os sistemas de vigilância de estabelecimentos comerciais, ou até mesmo os constantes monitoramentos realizados por funcionários, não tem o condão de impedir totalmente a consumação do crime"*.

---

[54] CUNHA, Rogerio Sanches. **Manual de Direito Penal:** Parte Especial. 9. ed. Salvador: Editora Juspodivm, 2017. p. 273-274.

[55] Artigo 155 do Código Penal: "Furto. Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel: Pena - reclusão, de um a quatro anos, e multa.
§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico."

[56] AZEVEDO, Marcelo André de; SALIM, Alexandre**. Direito Penal**: Parte Especial. 7. ed. Salvador: Editora Juspodivm, 2018. p. 312.

O furto majorado ou noturno caracteriza-se, pelos termos do parágrafo 1° do artigo 155 do Código Penal, por aquele cometido no período em que as pessoas normalmente então dormindo. Deve-se analisar os hábitos do local onde foi praticado. A maior reprovabilidade é em função de o agente ter maior facilidade no cometimento do crime, já que as chances de defesa da vítima, em termos de vigilância, estão diminuídas.

Já as qualificadoras estão previstas nos §§4°,5° e 6° do artigo supramencionado. Não será objeto de apreciação individual de cada uma delas na presente tese de conclusão de curso, mas ficam as palavras de Nelson Hungria sobre a reprovabilidade aumentada, e, portanto, justificadora de uma maior cominação legal em relação ao crime de furto[57]:

> "notadamente, quanto ao modo de execução, o furto pode revestir-se de circunstâncias eu lhe imprimem um cunho de maior gravidade, por isso que traduzem um especial *quid pluris* no sentido de frustrar a vigilante defensa privada da propriedade. Tais circunstâncias taxativamente enumeradas pela lei, entram, então, a funcionar como condição de maior punibilidade" (agravantes especiais, majorantes, qualificativas), e o furto se diz qualificado." (Ob. Cit.,v.7, p38.)

3.2 CRIMES DIGITAIS PUROS OU MISTOS

Há, na doutrina, diversas definições do que seria o crime puro de informática. Em linhas gerais, pode ser definido como crime que tem, por meio da conduta ilícita, o objetivo único e exclusivo de afetar, gerar dano, a um sistema de computador e seus dados contidos, utilizando-se de conhecimentos técnicos para tal.[58]

Outra definição, mais abrangente, é do Marco Aurélio Costa, segundo o qual crimes de informática são:

> "crimes de informática são aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas. Entendemos serem os elementos que compõe a informática o "software" e "hardware" (computadores e periféricos), os dados e sistemas contidos no

[57] AZEVEDO, Marcelo André de; SALIM, Alexandre**. Direito Penal**: Parte Especial. 7. ed. Salvador: Editora Juspodivm, 2018. p. 314.

[58] LICKS, Otto Banho; JUNIOR, João Marcelo de Araújo. **Aspectos penais dos crimes de informática no Brasil**. *In*: Revista dos tribunais Rio Grande do Sul, 1994. p. 95.

> computador e os meios de armazenamento externo, tais como: fitas, disquetes, etc. Portanto, são aquelas condutas que visam exclusivamente violar o sistema de informática do agente passivo"[59]

Em suma, quanto à tentativa de se fazer uma definição apropriada para o tema, pode-se dizer que se trata de qualquer conduta típica, antijurídica, e culpável, feita por meio de dispositivo informático contra outro dispositivo do mesmo tipo, tendo como alvo principal os seus dados, em qualquer forma que esteja disposto dentro do equipamento invadido.[60]

Conclui-se, então, que dois pontos devem estar presentes na conduta: ser feito por meio de aparelho informático; e ser exclusivamente contra dados.

Como foi dito anteriormente, o conceito de crime puro de informática, mesmo que tratado apenas de forma de doutrinária, tem repercussões no cenário atual, uma vez que, mesmo com a entrada em vigor da lei 12.737/12 no ordenamento jurídico brasileiro, ficou vago e incompleta a tratativa do que seria um crime deste gênero, e o que seria um crime comum, simplesmente praticado por meio da internet.

O rol da lei supramencionada acabou, aqui, por dispor sobre a conduta chamada de "furto de dados", distinguindo-o, de certa forma, do comum. Mesmo assim fica a dúvida sobre quando o objeto é considerado dado (e daí seria aplicada a pena prevista no artigo 154- A do Código Penal) e quando é considerado outra coisa, que permita caracterizá-la, seguindo os preceitos do tipo legal contido no artigo 155 do Código Penal, como furto.

Para Marcelo Crespo a distinção fica nítida. Os conceitos de cada um, mesmo antes da lei Carolina Dieckmann já tinha contornos bem definidos:

> **crimes digitais próprios ou puros** (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas.

---

[59] COSTA, Marco Aurélio. **Crimes de Informática III**. Retirado da Internet. Urugauiana, 1989. s/p.
[60] LICKS, Otto Banho; JUNIOR, João Marcelo de Araújo. **Aspectos penais dos crimes de informática no Brasil**. *In*: Revista dos tribunais Rio Grande do Sul, 1994. p. 97.

> **crimes digitais impróprios ou mistos** (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc.). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio.
> Simplificando, pode-se dizer que os crimes digitais são tanto os crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente reconhecemos como merecedores de proteção, praticados com auxílio da mais moderna tecnologia [...][61]

Decisões que mostram as divergências acima apresentadas serão aqui expostas e melhor explicadas, nos capítulos seguintes.

3.3 DA LEGALIDADE

O princípio da legalidade, previsto no artigo 5°, inciso II da Constituição Federal da República Federativa do Brasil, aqui, não será o norteador da tratativa, apesar da similaridade de nome daquele que será: Princípio da reserva legal ou da estrita legalidade.

Este está previsto no artigo 5°, XXXIX da CF, e também no art. 1° do Código Penal. É, portanto, cláusula pétrea, continuando a vigorar mesmo que, porventura, seja retirado do CP.[62] Dispõe que cabe a lei, exclusivamente, a criação de delitos e contravenções penais e a cominação de penas. Por este, extrai-se que, não há crime sem lei anterior que o defina, nem pena sem cominação legal.[63]

Para Cleber Masson, a história do princípio e seus objetivos se remetem à Carta Magna e à teoria da coação psicológica:

> "Seu mais seguro antecedente histórico se remete à Magna Carta de João Sem Terra, imposta pelos barões ingleses em 1215, ao estabelecer em seu art. 39 que nenhum homem livre poderia ser submetido à pena sem previa lei em

[61] CRESPO, Marcelo. **"As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos". Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.
[62] MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018. p. 25.
[63] GRECO, Rogério. **Curso de Direito Penal:** Parte Geral. v. 1. 16. ed. Rio de Janeiro: Impetus, 2014. p. 98.

> vigor naquela terra. Posteriormente o princípio da reserva legal (...) no com base em sua teoria da coação psicológica. Para ele, toda imposição de pena pressupõe uma lei penal. Somente a ameaça de um mal por meio da lei fundamenta a noção e a possibilidade jurídica da pena".

O princípio da reserva legal possui dois fundamentos, um de natureza jurídica e outro de caráter político. O jurídico se remete ao princípio da taxatividade, segundo o qual, a lei deve conter uma precisão no que é dito, não só em relação ao tipo penal, mas também à pena cominada que o acompanha.

Uma consequência lógica deste princípio é a vedação a analogia *in malam partem*, ou seja, para uma pior situação da parte ré. Isso, nas situações de vaco legislativo. Isso será melhor explanado logo a seguir. Para complementação da informação, o fundamento político é a proteção do ser humano diante da ação do Estado. São os direitos fundamentais de primeira geração.[64]

O resto da explanação sobre a legalidade e as formas possíveis de se fazer a intepretação de um tipo penal, será feita conjuntamente com a análise de jurisprudências firmadas em âmbito nacional, tanto de matérias relacionadas ao tema principal da presente obra, ligadas a crime de furto, quanto a matérias gerais de direito penal, relacionadas aos próprios princípios e regras.

[64] MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018. p. 26.

4 DA LEGISLAÇÃO PERTINENTE

4.1 LEI 12.737/12

Em 2013 entrou em vigor a Lei 12.737, alterando o Código Penal e trazendo a tipificação de condutas tratadas como delitos informáticos. Sua pretensão era a de tornar atos que não eram penalmente previstos na legislação, em condutas típicas.[65]

Foram criados os artigos 154-A e 154-B, trazendo ao Código Penal uma tratativa sobre a conduta "invasão de dispositivo informático". Também foram alterados os artigos 266 e 298 do presente diploma legal, que tratam, respectivamente da "interrupção, ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública" (onde houve um acréscimo de 2 parágrafos), e da "falsificação de documento particular". Nesse último foi equiparado ao disposto no caput, o cartão de crédito.

Esse dispositivo legal, que entrou em vigor em abril de 2013, foi apelidado de Lei Carolina Dieckmann, por ter sido aprovada próxima do acontecimento de vazamento na internet de imagens particulares da famosa atriz, por meio de invasão a dispositivo eletrônico, no caso, seu computador.

Sobre o bem tutelado pelo artigo 154-A do referido código, pode-se dizer que é o da privacidade, que engloba o direito à intimidade. O agente não possui qualquer qualidade específica tratando-se, portanto, de crime comum. Já o sujeito passivo deve ser o proprietário do dispositivo, ou aquele que tem a sua posse e faz uso desse.[66]

Sobre a elementar do tipo, o conceito de invasão deve ser considerado levando-se em consideração a realidade do meio em que se dá, no caso, o cibernético. Segundo Luiz Augusto Pessoa Nogueira:

---

[65] AGNOLETTO, Giovani Celso; BEZERRA, Clayton da Silva**. Combate ao crime cibernético**. Rio de Janeiro: Mallet, 2016. p. 23.

[66] AGNOLETTO, Giovani Celso; BEZERRA, Clayton da Silva**. Combate ao crime cibernético**. Rio de Janeiro: Mallet, 2016. p. 25.

> (...) "invadir, no sentido virtual ou cibernético, é todo ato, sem autorização, que, de forma física ou virtual, consegue acessar dispositivo físico ou informático, quer seja pelo uso da força ou coação, quer seja de modo ardiloso". Resumindo, entrar em um dispositivo ou um sistema sem autorização do proprietário. " [67]

Já a expressão "dispositivo informático", trata-se de todo equipamento que tenha a capacidade de se conectar, não só à rede mundial de computadores ou internet, mas também a todos os aparelhos por meio do qual se pode processar dados. Exemplos são os smartphones e os chamados equipamentos periféricos, como pendrive e impressora.

Por poder ser "conectado ou não à rede de computadores" há um maior alcance do que se fosse apenas para o caso de conexão à internet. Tal abrangência não se verifica no termo "mediante violação indevida de mecanismo de segurança", já que, a partir desta disposição, chega-se à conclusão de que deve haver algum mecanismo de segurança que impeça o acesso ao conteúdo do dispositivo informático.

O elemento subjetivo é o dolo previsto no artigo, isto é, deve haver a intenção de obter adulterar ou destruir dados ou instalar vulnerabilidades para obter vantagem ilícita. No entanto, entende-se que para a sua consumação, sendo o crime formal, basta que haja a invasão ao dispositivo informático. O sucesso do fim específico supracitado trata-se, portanto, de mero exaurimento do crime.[68]

Sobre esse mesmo tema, outra parte da doutrina entende de forma diferente. Para Marcelo Crespo o termo invadir possui outra conotação, sendo necessário o real dado ao bem.

> "Invadir" sugere que o dispositivo informático objeto do crime seja acessado mediante violação de mecanismo de segurança, que poderá ser uma senha ou um firewall. Por isso a redação nos soa redundante, haja vista que sem a superação de uma barreira não há que se falar em invasão, mas de acesso. E, nesta perspectiva, haverá crime impossível por impropriedade do objeto, caso o dispositivo se encontre desprotegido.[69]

---

[67] Ibidem. p. 26.
[68] Idem.
[69] CRESPO, Marcelo. **"As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos". Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.

A tentativa é possível de se configurar. Ocorre quando, por motivos alheios à vontade do agente, este não consegue invadir o dispositivo, seja por imperícia no rompimento da barreira do sistema de segurança, seja por qualquer outro motivo.

Passando ao parágrafo 1° do artigo 154-A do Código Penal (introduzir no rodapé), há a previsão de equiparação, de grande relevância para o cenário atual de crimes mais perpetrados no Brasil, ao crime de "invasão de dispositivo informático", a produção e disponibilização de programa de computador, com o intuito do previsto no caput. Ou seja, produção de hardware e software. O hardware mais utilizado atualmente nesse sentido, é o chamado "chupa-cabra".[70]

O parágrafo segundo do artigo traz uma causa de aumento de pena, para o caso de, do delito, houver prejuízo econômico para a vítima. Aqui, prejuízo econômico relacionado a danos de ordem material e lucros cessantes, diante do impedimento de exercício profissional. O terceiro parágrafo trata da hipótese de invasão de dispositivo e obtenção de segredos de comerciais e industriais.

Tal paragrafo tem a cominação legal do caput aumentada, tratando-se, por tanto, de forma qualificada. Por último, ainda sobre este, vale fazer uma distinção entre o previsto no artigo 10 da Lei 9296/96 e ele. No primeiro, há a obtenção de dados e informações após a interceptação, enquanto no segundo isto é feito a partir da coleta dos dados já arquivados no dispositivo invadido.

O parágrafo 4° traz uma causa de aumento de pena específica (relacionada ao parágrafo anterior). Já o 5°, uma causa de aumento de pena se praticado contra vítimas com qualidades específicas.

O artigo 154-B do Código penal trata do tipo de ação penal do crime previsto no artigo anterior. Aqui, se não for contra a administração pública, direta ou indireta, será somente por meio de representação, ou seja, ação penal pública condicionada.

[70] Ibidem. p. 27-28.

Por mais relevantes que sejam os outros artigos alterados e as novas disposições trazidas pela lei 12.737/12, o objeto do presente estudo está restrito ao que foi exposto acima, e por isso, não será analisado, de forma pormenorizada, como foi até aqui, o resto do dispositivo legal.

Ainda dentro da tratativa desta lei, vai destacar uma que seguia no mesmo caminho, mas teve um esvaziamento de seu conteúdo, tanto por causa dos trâmites para sua aprovação, quanto por causa da própria redação da lei, que exigia demais dos provedores.

Marcelo Crespo, em um dos seus artigos comenta sobre a lei 12.735, mais conhecida como lei Azeredo:

> [...] enquanto projeto foi apelidada de "AI-5 digital" por conta dos pontos polêmicos que continha, em especial, os referentes à guarda dos logs de acesso dos usuários pelos provedores. Em face disso o projeto foi esvaziado e se tornou uma lei com poucas e frágeis disposições. Em resumo, o texto aprovado determina que os órgãos da polícia judiciária deverão criar delegacias especializadas no combate a crimes digitais (art. 4º). A medida é salutar, mas depende do Poder Público a ela prover a concretude necessária, investindo na especialização da Polícia com treinamentos e equipamentos. Ainda não se pode dizer que as delegacias que foram criadas estão plenamente aptas a prover o atendimento adequado às vítimas de crimes digitais.[71]

Nesse interim, é válido tecer algumas considerações acerca do acordão do resp. 121428 RJ 1997/0014040. Trata-se de um recurso especial, no qual a parte recorrente, com base nas alíneas e c , do inciso III, do art. 105, da Constituição da República, interpôs o recurso contra acórdão do Tribunal de Justiça do Rio de Janeiro que entendeu que a lista de serviços anexada ao Decreto-lei n.º 406/68 não apresentava taxatividade absoluta, sendo esta passível de interpretação extensiva ou analógica.

Defendeu, a recorrente, que a lista de serviços era taxativa, não permitindo interpretação extensiva, de forma que os serviços tributados pela recorrida seriam indevidos por não estarem relacionados nesse rol.

---

[71] CRESPO, Marcelo. **"As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos". Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.

O ministro Relator, que teve seu voto acompanhado por unanimidade na Corte, dispôs pela improcedência do recurso, pelo fato de estar havendo, no caso, interpretação analógico- extensiva, como segue:

> Na hipótese, entendo não haver qualquer ofensa ao art. 108, 1º, do CTN. A regra em destaque veda o emprego da analogia para a cobrança de tributo não previsto em lei. O que se tem, no caso dos autos, é o recurso à interpretação extensiva autorizada pela própria norma de tributação, já que muitos dos itens da lista de serviços apresentam expressões do tipo "congêneres", "semelhantes", "qualquer natureza", "qualquer espécie", dentre outras tantas, as quais deixam claro que o intuito do legislador foi o de tributar o gênero, abarcando todas as suas espécies.
>
> Assim, prevendo o legislador complementar a impossibilidade de fixar todas as espécies e derivações de um mesmo serviço, preferiu tributar o gênero, estabelecendo, ao final de cada item, uma cláusula que permite ao aplicador do direito o recurso à interpretação extensiva.

E complementa ainda, tratando da distinção entre interpretação analógico – extensiva da analogia:

> Diga-se, ainda, que não se pode confundir analogia com interpretação analógica ou extensiva. A analogia é técnica de integração, vale dizer, recurso de que se vale o operador do direito diante de uma lacuna no ordenamento jurídico. Assim, na ausência de norma, vedado o non liquet , deverá o magistrado aplicar a analogia para não deixar o jurisdicionado sem resposta e a lide sem solução. Já a interpretação, seja ela extensiva ou analógica, objetiva desvendar o sentido e o alcance da norma, para então definir lhe, com certeza, a sua extensão. A norma existe, sendo o método interpretativo necessário, apenas, para precisar-lhe os contornos.

Tal interpretação não deve prosperar, no entanto, para o regramento do direito penal. Isso porque, em primeiro lugar, a interpretação da lei penal possui suas nuances.

Quanto ao seu sujeito, pode ser dito que se subdivide em três classificações: autêntica; judicial; e doutrinária. Para os fins deste estudo, a judicial se destaca, sendo a interpretação aplicada pelos membros do Poder Judiciário, na tentativa de resolução de litígios que lhes são submetidos.[72]

No que diz respeito ao resultado dessa interpretação, pode ser: declaratória; extensiva; e restritiva. Na declaratória há uma sintonia exata entre o texto da lei e a vontade do legislador no momento de sua elaboração. Na restritiva a lei deve ter um

[72] MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018. p. 26.

alcance reduzido, em sua interpretação. Já na extensiva, ocorre quando deve haver uma correção da disposição legal, por ser mais estreita do que deveria. Amplia-se, portanto, o texto da lei.

Tal ampliação não pode, no entanto, resultar em interpretação extensiva feita para pior. Há firmamento, inclusive, de que em matéria penal, não pode ser feito de jeito algum, em respeito ao princípio da reserva legal, conforme RHC 85.217-3/SP:

> HABEAS CORPUS. PRISÃO PROVISÓRIA. CONTAGEM PARA EFEITO DA PRESCRIÇÃO. IMPOSSIBILIDADE. O tempo de prisão provisória não pode ser computado para efeito da prescrição, mas tão-somente para o cálculo de liquidação da Pena. O artigo 113 do Código Penal, por não comportar interpretação extensiva nem analógica, restringe-se aos casos de evasão e de revogação do livramento condicional. Recurso ordinário em HC a que se nega provimento.
> (STF - RHC: 85217 SP, Relator: EROS GRAU, Data de Julgamento: 02/08/2005, Primeira Turma, Data de Publicação: DJ 19-08-2005 PP-00047 EMENT VOL-02201-3 PP-00439 LEXSTF v. 27, n. 321, 2005, p. 431-435 RB v. 17, n. 503, 2005, p. 32-33 RTJ VOL-00194-03 PP-00960)

Vale dizer a interpretação analógica consiste em possibilitar ao aplicador da lei, fazer uma interpretação do tipo penal que tem casos inúmeros e imprevisíveis quando da formulação da lei.

A analogia, por sua vez, só pode ser utilizada, no direito penal, para normas não incriminadoras. Isso porque, trata-se de método de integração, e não de interpretação da lei penal. Nesse caso não há nem mesmo uma lei para ser interpretada. Essa vedação se dá em respeito ao preconizado pelo princípio da estrita legalidade.[73]

Agora, trazendo uma decisão recente, em um conflito de competência negativo, a 3ª Seção do STJ firmou entendimento no sentido de que a subtração de valores de conta corrente mediante transferência eletrônica fraudulenta configura crime de furto, como o que consta no artigo 155, parágrafo 4°, inciso II, do Código Penal.[74]

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSUAL PENAL. FURTO MEDIANTE FRAUDE. TRANSFERÊNCIA

[73] MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018. p. 26.
[74] REVISTA CONSULTOR JURÍDICO. **"STJ divulga jurisprudência sobre conceitos de crimes pela internet"**. Disponível em: <https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet>. Acesso em: 20 jun. 2018.

> BANCÁRIA VIA INTERNET SEM O CONSENTIMENTO DA VÍTIMA. CONSUMAÇÃO NO LOCAL DA AGÊNCIA ONDE O CORRENTISTA POSSUI A CONTA FRAUDADA. COMPETÊNCIA DO JUÍZO SUSCITADO. 1. A Terceira Seção desta Corte Superior firmou o entendimento no sentido de que a subtração de valores de conta corrente, mediante transferência fraudulenta, utilizada para ludibriar o sistema informatizado de proteção de valores, mantidos sob guarda bancária, sem consentimento da vítima, configura crime de furto mediante fraude, previsto no art. 155, § 4º, inciso II, do Código Penal - CP. 2. O delito em questão consuma-se no local da agência bancária onde o correntista fraudado possui a conta, nos termos do art. 70 do Código de Processo Penal - CPP; no caso, na Comarca de Barueri/SP. Conflito de competência conhecido para declarar competente o Juízo de Direito da 1ª Vara Criminal de Barueri/SP, o suscitado.
> (STJ - CC: 145576 MA 2016/0055604-1, Relator: Ministro JOEL ILAN PACIORNIK, Data de Julgamento: 13/04/2016, S3 - TERCEIRA SEÇÃO, Data de Publicação: De 20/04/2016)

Não só por este, mas em outros entendimentos da Cortes superiores da Justiça, está prevalecendo o que vai ao encontro de Marcelo Crespo, que defende a ideia da existência de crimes puros e crimes mistos de informática. Conforme já foi dito aqui, mas se faz necessário repetir para não perder o encadeamento do raciocínio, tais crimes se diferenciam:

> crimes digitais próprios ou puros (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os sistemas informáticos e os dados. São também chamados de delitos de risco informático. São exemplos de crimes digitais próprios o acesso não autorizado (hacking), a disseminação de vírus e o embaraçamento ao funcionamento de sistemas.
> crimes digitais impróprios ou mistos (condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc.). São exemplos de crimes digitais impróprios os contra a honra praticados na Internet, as condutas que as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil, o estelionato e até mesmo o homicídio.[75]

A divergência, no entanto, se fazia presente na doutrina. Quanto a um dos objetos do presente de estudo, o furto de dados, acabou restando prejudicada a discussão, quanto à legalidade, ou não, dessa.

---

[75] CRESPO, Marcelo. **"As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos". Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.

Isso porque, a redação do Caput do artigo 154-A do Código Penal dispôs exatamente sobre a invasão com o intuito de obtenção de dados. Para grande gama dos demais delitos, no entanto, a divergência continua.

Antes da edição da lei, Marcelo Crespo, com sua Obra "Crimes Digitais" figurava, nesse ponto, no lado oposto ao dos que defendiam a desnecessidade de edição de lei específica para punir condutas praticadas pelo meio digital.

Uma das expoentes, que encabeçava a linha neste sentido, era Rita de Cassia que, sem fazer distinção entre crimes puros e impuros, sustentava que danos ou alterações de dados poderiam sim integrar a esfera dos crimes contra o patrimônio, uma vez esses dados expressam quantias que possuem valor no mundo real, gerando, caso prejudicadas, supressão de quantia de uma conta bancária.[76] Nas suas palavras:

> "Aponta-se para uma revolução nas coisas do mundo, em que se está passando dos átomos para os bits. (…) Dentro das relações jurídicas reguladas por átomos, tem-se que, no furto de coisa, coisa é um conjunto de átomos. (…) Um dos problemas para se negar a prática do furto por meio do sistema informático reside no fato de não se reconhecer na informação armazenada um bem material, mas sim imaterial e, como tal, insuscetível de apreensão como objeto, negando-se-lhe a condição de coisa. Mas a informação, neste caso, por se tratar de patrimônio, refere-se a bem material, apenas grafado por meio de bits, suscetível, portanto, de subtração. Assim, ações como alteração de dados referentes ao patrimônio, com a supressão de quantia de uma conta bancária, pertencem à esfera dos crimes contra o patrimônio" (SILVA. 2003, p. 97)

Já Marcelo Crespo, apontava que isso não era possível, já que deve-se respeitar o princípio da reserva legal, disposto nos artigos 5°, inciso XXXIX da Constituição Federal e 1° do Código Penal. Por este, a lei deveria, caso quisesse abarcar o dado digital como um bem móvel, passível de subtração, deveria ser feita alteração legislativa, para evitar-se a interpretação analógico extensiva *in malam partem*, ou seja, para uma pior situação do acusado.

Isso, como foi feito na edição do parágrafo 3° do Código Penal, no qual se equiparou a bem móvel a energia elétrica. Até lá, qualquer dano não deveria ser tratado como algo penalmente relevante, e sim, algo a se tratar na esfera cível.

---

[76] TANGERINO, Dayane Fanti. "Direito Penal e Novas Tecnologias". **Canal Ciências Criminais**. Jan. 2016. Disponível em: <https://canalcienciascriminais.com.br/direito-penal-e-novas-tecnologias/>. Acesso em: mar. 2018.

Apesar de seu pensamento continuar para outros bens juridicamente relevantes e tutelados pelo direito, com a edição de lei 12.737/12, o bem dado digital, agora é sim tutelado contra a sua subtração. Isso, com algumas ressalvas, tratadas não só por doutrinadores que enxergaram essa nova possibilidade, mas também Marcelo Crespo.

4.2 CRÍTICAS à LEI 12.737/12

Após a entrada em vigor da lei 12.737/12, mais conhecida como lei Carolina Dieckmann, algumas críticas surgiram, tanto quanto a efetividade da lei, no seu cumprimento principal do objetivo de punir aqueles que cometem os delitos previstos por ela e coibir aqueles que potencialmente os fariam, quanto em sua parte técnica.

Muito é dito de isto ter ocorrido porque foi fruto da lógica da política contemporânea brasileira, de atender, às pressas, anseios populares e pressões midiáticas a partir da edição de leis.[77]

A primeira das críticas a se fazer é a que ocorre diante da problemática já na fase de investigação criminal. Ali, a autoridade policial, ao solicitar, a provedores de conteúdo ou de conexão, informações cadastrais sobre usuários, a partir dos seus registros de IP (meio pelo qual se tem controle do canal de envio e do de recebimento de certo dado, imagem ou informação, como explanado em maiores detalhes no capitulo inicial da presente obra), tem grandes dificuldades de receber um resultado rápido e positivo. Acontece, normalmente, de deparar-se com um servidor que não armazenou as informações, ou a fez de forma incorreta e incompleta.

Algumas das implicações negativas, nesses casos, são a não resolução das investigações, e o arquivamento do inquérito pelo Ministério Público. Por não prever procedimentos especiais para esse tema, de crime praticado no meio cibernético, a legislação busca auxílio no Marco Civil da Internet.

---

[77] RIBAS JUNIOR, Douglas. **Lei Carolina Dieckmann e o sistema penal brasileiro.** Canaltech (site). Disponível em: < https://canaltech.com.br/juridico/Lei-Carolina-Dieckmann-e-o-sistema-penal-brasileiro/>. Acesso em: mai. 2018.

Esse, apesar de não ser o ideal para a resolução dos conflitos existentes no âmbito penal, dão algum suporte, ao estabelecer, com obrigatoriedade, aos usuários e provedores que atuem de acordo com deveres e garantias. Dentre elas, está a imposição de que os provedores devem manter registro de dados sobre datas e horários, por exemplo. É o chamado “guarda de logs”.

Isso é de suma importância para a resolução de investigações norteadas pelo crime contido no artigo 154-A do Código Penal. O tempo pelo pelo qual fica o provedor obrigado a guardar esses logs é, no entanto, irrazoável, o que gera uma ineficácia do regramento, já que os provedores se veem obrigados a descumprir com a norma. Isso é fruto, também, de uma lei feita às pressas. O Marco Civil da Internet foi editado em meio a escândalos mundiais de espionagem norte-americana a governos (inclusive o brasileiro) e um ambiente cibernético sem lei que pudesse coibir ações do tipo.

Como foi apresentado no capítulo anterior, a lei 12.737/12, além de não apresentar procedimentos processuais (se limitando a tratar de parte material), fez poucas e insuficientes previsões penais, permitindo que haja, ainda hoje, um grande número de condutas danosas à sociedade que se encontram na situação de atipicidade(citar um exemplo- como estupro cibernético).

Ainda assim, em mais um ponto de crítica à redação da lei, no que diz respeito ao contido no artigo 154-A, que trata da invasão de dispositivo informático e contém a ideia do chamado “furto de dados”, chega quase a ser ineficaz, tanto no objetivo de punição estatal frente à prática de um ilícito penal, quanto à inibição daqueles que pretendem fazê-lo, tamanha é a inexpressividade da pena cominada em abstrato. É de detenção, de 3 meses a 1 ano e multa, sendo considerada prática de menor potencial ofensivo.

Outro importante ponto a ser tratado é em sentido contrário ao exposto até o momento. Da persecução penal, olha-se, de outro lado, pela real necessidade de se buscar punição para aquele que simplesmente invade um dispositivo informático.

Quando constatada a insignificância, seguindo precedente do STF, deve-se excluir a tipicidade, pela ausência da sua vertente material:

> "O princípio da insignificância qualifica-se como fator de descaracterização material da tipicidade penal. O princípio da insignificância – que deve ser analisado em conexão com os postulados da fragmentariedade e da intervenção mínima do Estado em matéria penal – tem o sentido de excluir ou de afastar a própria tipicidade penal,examinada na perspectiva de seu caráter material."
> (RHC 122.464/BA, rel. Min Celso de Mello, 2.ª Turma, j. 10.06.2014.)

Ressaltando que só incorre em tal tipo penal aquele que rompe, para adentrar nesse dispositivo, com barreira, sistema de segurança que vise impedir o acesso aos dados contidos no dispositivo. Caso contrário, configura-se atípica a conduta.

Até mesmo nesse ponto, a lei falta com a técnica, ao não definir que tipo de dispositivo ou sistema de segurança seria esse. Fica o questionamento, ainda doutrinário se esse seria algum tipo de firewall ou se a exigência de uma simples senha para o acesso seria o suficiente para tal.

A consumação do ato se dá no mero ato de invasão, quando poderia, seguindo o princípio da fragmentariedade, caracteriza-se somente quando da ocorrência real de tentativa ou prática de crimes já previstos no ordenamento, como extorsão[78] ou o próprio furto.

Então, no caso de uma pessoa, que se encontra em seu ambiente de trabalho, e acaba deixando seu dispositivo informático (celular ou computador) sem qualquer bloqueio, não tem tipo penal configurado caso o seu amigo acesse suas informações e dados, mesmo contra a vontade do proprietário.[79]

---

[78] Artigo 158 do Código Penal: "Extorsão. Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
Pena - reclusão, de quatro a dez anos, e multa.
§ 1º - Se o crime for cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade.
§ 2º - Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior.
Vide Lei nº 8.072, de 25.7.90
§ 3o Se o crime for cometido mediante a restrição da liberdade da vítima, e essa condição é necessária para a obtenção da vantagem econômica, a pena é de reclusão, de 6 (seis) a 12 (doze) anos, além da multa; se resulta lesão corporal grave ou morte, aplicam-se as penas previstas no art. 159, §§ 2o e 3o, respectivamente. (Incluído pela Lei nº 11.923, de 2009)"

[79] BERETTA, Pedro. "**Sem meios eficazes, Lei Carolina Dieckmann até atrapalha"**. Revista do Consultor Jurídico (online). Disponível em: <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>. Acesso em: mai. 2018.

Por último, pode-se dizer que, novamente, a má-redação do texto penal talvez tenha prejudicado o público em geral. A lei 12.737/12 pretendeu, como se extrai da leitura do parágrafo 1° do artigo 266 do Código Penal, parágrafo este trazido pela lei supramencionada. Por ele, passa a ser punível penalmente o "Denial of Service", ou "denegação de serviço".

Trata-se de punir penalmente aquele que interromper ou perturbar serviços telegráfico, informático, telemático, ou de informação de utilidade pública. Ao ressalvar para apenas os atos que prejudiquem o funcionamento do que é de utilidade pública, o tipo penal ficou restrito a uma parcela muito pequena de hipóteses, e deixou de abarcar todo e qualquer serviço particular que não seja considerado de utilidade pública.[80]

[80] CRESPO, Marcelo. **"As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos". Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.

CONSIDERAÇÕES FINAIS

Depois de tratada toda a temática pertinente ao tema, abordando tanto informações imprescindíveis para a continuidade do raciocínio, quanto as aquelas que tangenciam o principal, mas servem como “escora”, funcionando como suporte teórico e contextual dos cenários do Brasil e do Mundo, desde a década de 60 até os dias atuais, agora é chegada a hora de uma conclusão lógica.

Apesar desta ter sido construída a partir de todo o desenvolvimento do presente estudo, sendo dita pouco a pouco nas entrelinhas, o espaço final para ela se faz necessário, como uma oportunidade de recapitulação e aglutinação do que foi dito e fundamentado, às vezes em um sentido, às vezes no contrário.

A história do surgimento e evolução da internet foi importante para que se pudesse ter uma dimensão do espaço onde o tema principal se perpetua. Conceitos básicos foram apresentados durante a exposição, e a rede mundial de computadores foi caracterizada desde o seu ponto mais elementar, como a sua conceituação (um complexo de diversas redes, com objetivo final de permitir a troca de dados entre os usuários), até seus termos mais sofisticados, como o funcionamento do código binário que compõe, e os estudos feitos para se chegar onde está.

Dados foram trazidos, mostrando a fragilidade dos países em lidar com a recente problemática, em especial, o Brasil, que além de ter um dos maiores números de casos de malwares danificando aparelhos informáticos dos seus usuários, não tem (já antecipando uma conclusão tardia) sequer legislação realmente pertinente e satisfatória para resolução de qualquer parte desse novo desafio.

Lei editada às pressas, com objetivo político somente que, se algo trouxe de benéfico, foi o aumento das discussões sobre o tema, e inclusive grande responsável por fomentar o presente trabalho de conclusão de curso.

Voltando à digressão, foi tratada a questão do direito fundamental à privacidade. Por José Afonso da Silva, privacidade é “o conjunto de informações acerca do indivíduo que ele pode decidir manter sob o seu exclusivo controle, ou comunicar, decidindo a

quem , quando, onde e em que condições, sem isso pode ser legalmente sujeito", e Marcelo Crespo faz saltar aos olhos a nova prática de empresas, que vendem informações de seus usuários para terceiros usarem da forma que quiserem, evidenciando uma grande violação os direitos à privacidade, a partir de políticas agressivas de "cookies".

Outro ponto tratado logo a seguir foi o da jurisdição nos casos dos crimes perpetrados por meio da internet. Uma decisão muito pertinente ao nosso tema, por um acaso, foi feita no mês de junho deste ano, pelo Superior Tribunal de Justiça, em que decidiu um conflito negativo de competência por crime praticado em um Estado, e que teve resultado em outro.

A prática foi justamente a tida como "furto bancário", no qual há subtração de valores a partir da alteração de dados bancários. Foi decidido o impasse após haver a desclassificação do crime de estelionato, tipificado pelo artigo 171 do CP, para o de furto qualificado, presente no artigo 155, §4°, inciso II do mesmo diploma legal. Acabou por ser decidido que o local competente é definido por onde houve a subtração do bem da vítima, ou seja, do local onde ela se encontrava.

O tema foi abordado, superada a fase da jurisdição, a partir do estudo do perfil dos agentes dos crimes em questão. Trata-se de um novo criminoso, que se utiliza de ferramentas de alta tecnologia, e não se expõe, buscando no anonimato atingir seus objetivos, sejam eles políticos ou, como o usual, financeiros. Diversas espécies do gênero Hacker foram trazidas e explicadas, superando dificuldades existentes quanto aos perfis de cada um deles e suas diferentes áreas de atuação.

Alguns deles, como o cracker e o próprio conceito de hacker merecem ser destacados. O primeiro trata-se do tipo de hacker que gera mais danos aos dispositivos ligados à rede mundial e computadores. Suas motivações são vantagens econômicas e o reconhecimento de atuantes da área do tamanho de suas habilidades. Isso é atingido por meio da invasão de sistemas com avançados mecanismos de segurança.

Já o hacker, apesar de receber a fama do supramencionado, é o gênero deste, tendo várias espécies. O que é comum a todos, é a característica de ser um especialista

em informática, que atua no sentido de descobrir defeitos nos mecanismos de segurança para dispositivos informáticos.

Após seguir tangenciando por áreas periféricas, para adentrar no tema principal com o suporte necessário, essa passa a ser abordado, trazendo, a presente obra, os principais apontamentos da doutrina quanto ao crime previsto no Caput do artigo 155 do Código Penal: o furto.

A questão da conceituação do crime puro de informática e a sua distinção do crime comum é feita no capítulo seguinte. Está tratativa mostrou-se muito importante para o próprio encadeamento lógico do tema. Por ele foi visto que o crime puro tem como alvo os próprios dados em si, enquanto para o crime comum (impróprio ou misto), o ataque feito por meio digital, mas para praticar condutas já tipificadas pelo ordenamento jurídico brasileiro, e que também podem se perpetuar fora do meio digital.

Essa distinção dá embasamento teórico para a explicação de parte da decisão do STJ em um caso de conflito de competência(CC: 145576 MA 2016/0055604-1), exposta e tratada na parte “da legalidade”, na qual o crime de “furto bancário”, feito a partir de alteração de dados via internet, foi considerado como conduta prevista no artigo 155, parágrafo 4°, inciso II do Código Penal: o crime de furto qualificado, mediante fraude (e não tipificado no artigo 154-A, que abarca, de certo modo, o chamado “furto de dados”).

Após seguir tangenciando por áreas periféricas, para adentrar no tema principal com o suporte necessário, esta passa a ser abordado com ainda mais clareza, trazendo, a presente obra, os principais apontamentos da doutrina quanto ao crime previsto no Caput do artigo 155 do Código Penal: o furto.

Com todas as suas nuances, desde a sua conceituação e análise do tipo penal, até a sua conexão com o crime de “furto de dados”, que está previsto no artigo 154-A do Código Penal.

Essas considerações, por si só, já serviram de parâmetro para a supracitada conduta, que está presente na lei 12.737/12, que alterou o Código Penal. No crime de

furto, diversos pontos controversos já foram definidos, ou ao menos bem discutidos pela doutrina e pelas Cortes do país.

No caso da consumação, por exemplo, adota-se para o furto a corrente do amotio, sendo considerado, então, consumado o crime de furto quando o proprietário do bem perde o contato, ou a opção de fazê-lo, com o bem móvel, independendo se isso se deu por causa da mudança de lugar deste pelo agente, seja por ele o destruiu ou deixou a salvo.

No crime contra dados não há a mesma certeza. Parte da doutrina, como Marcelo Crespo, defende que ocorre quando há lesão aos dados ou à informação contida no dispositivo informático invadido. Já por outra parte da doutrina, isso já ocorre no momento em que o dispositivo é invadido, sendo o resto da conduta prevista no elementar do tipo, como mero exaurimento deste.

Outro ponto é quanto ao objeto em si alvo da tutela penal desse tipo penal. Nelson Hungria, defende que esse é a propriedade. E no delito do artigo 154-A do CP? Por parte da doutrina é a liberdade individual, já que consta neste capítulo, e não em algum do título dos crimes contra o patrimônio.

Em mais uma diferença, Rogério Sanches aponta que o objeto material do crime de furto deve ser, coisa alheia móvel, e economicamente apreciável. Outra parte da doutrina o rebate, afirmando que não necessariamente precisa ser economicamente apreciável. Defendem poder ser algo de valor sentimental.

Quanto aos dados, a discussão não avança até esse ponto. Fica pela problemática poder considerar ou não, “dados” como coisa alheia móvel. Se sim, vale dizer, deveria ser enquadrado no crime de furto, e não em um diferente.

Tal discussão fomenta o debate sobre toda essa questão. Essa é, para alguns, um dos únicos pontos positivos da lei 12.737/12, mais conhecida como lei Carolina Dieckmann.

De outro modo, as críticas a esse dispositivo são grandes, e aqui, numa conclusão final, devem ser destacadas. A problemática já se inicia na fase de investigação criminal. A autoridade policial, quando requer, informações cadastrais sobre usuários, a partir dos seus registros de IP tem grandes dificuldades de receber um resultado rápido e positivo.

Isso porque não houve qualquer disposição sobre procedimento, na lei. Resumiu-se a tratar de questões materiais. Tem- se, então, o cenário onde a legislação, para resolução da questão, busca auxílio no Marco Civil da Internet, quando o crime é praticado no meio cibernético.

A lei 12.737/12, além de não apresentar procedimentos processuais (se limitando a tratar de parte material), fez poucas e insuficientes previsões penais, permitindo que haja, ainda hoje, um grande número de condutas danosas à sociedade que se encontram na situação de atipicidade

Em mais um dos pontos negativos é disposto que, no artigo 154-A, que trata da invasão de dispositivo informático e contém a ideia do chamado “furto de dados”, chega quase a ser ineficaz, tanto no objetivo de punição estatal frente à prática de um ilícito penal, quanto à inibição daqueles que pretendem fazê-lo, tamanha é a inexpressividade da pena cominada em abstrato. É de detenção, de 3 meses a 1 ano e multa, sendo considerada prática de menor potencial ofensivo.

Outro importante ponto a ser tratado é em sentido contrário ao exposto até o momento. Da persecução penal, olha-se, de outro lado, pela real necessidade de se buscar punição para aquele que simplesmente invade um dispositivo informático, e é trazida decisão do STF quanto a atipicidade da conduta quando for caso em que o princípio da insignificância se faz presente.

A consumação do ato se dá no mero ato de invasão, quando poderia, seguindo o princípio da fragmentariedade, de caracterizar-se somente quando da ocorrência real de tentativa ou prática de crimes já previstos no ordenamento, ou a própria obtenção dos dados ou outros elementares do tipo (também previstas no artigo 154-A do CP).

Terminando a lista dos problemas ainda persistentes com o advento desta lei, e dos novos traídos por ela, foi dito sobre a falta com a técnica, ao não se definir que tipo de dispositivo ou sistema de segurança seria esse. Fica o questionamento, ainda doutrinário, se esse seria algum tipo de firewall ou se a exigência de uma simples senha para o acesso seria o suficiente para tal.

Por último, a lei 12.737/12, que pretendeu, como se extrai do parágrafo 1° do artigo 266 do Código Penal, punir a conduta do "Denial of Service", ou "denegação de serviço", acabou, por má-opção de redação, tornando-o quase ineficaz.

Isso porque. Este trata-se de trata-se de punir penalmente aquele que interromper ou perturbar serviços telegráfico, informático, telemático, ou de informação de utilidade pública. Ao ressalvar para apenas os atos que prejudiquem o funcionamento do que é de utilidade pública, o tipo penal ficou restrito a uma parcela muito pequena de hipóteses, e deixou de abarcar todo e qualquer serviço particular que não seja considerado de utilidade pública.

Diante de todo o exposto, conclui-se que o crime de furto, propriamente dito, quando praticado por meio digital, ou da internet, vem sendo tido pelas Cortes do país como admissível, típico. A internet, como um instrumento qualquer, apenas é ferramenta do delito.

O furto bancário, crime de maior expressividade em termos de danos, considerando todos os outros crimes praticados por meio virtual, é tipificado como o descrito no artigo 155, parágrafo 4°, inciso II (furto qualificado, por meio de fraude).

Já o crime puro de informática descrito como "furto de dados" ainda é muito lacunoso, tendo o ordenamento jurídico o dever de resolver tal problemática, a partir de legislação adequada para o tema. A lei 12.737/12 não se mostrou eficiente, permitindo que condutas penalmente relevantes se travistam de figuras atípicas.

REFERÊNCIAS BIBLIOGRÁFICAS

AGNOLETTO, Giovani Celso; BEZERRA, Clayton da Silva**. Combate ao crime cibernético**. Rio de Janeiro: Mallet, 2016.

AGRELA, Lucas. **"Grupo Anonymous ataca Temer e apoia greve dos caminhoneiros".** Revista Exame (online). Disponível em: < https://exame.abril.com.br/tecnologia/grupo-anonymous-ataca-temer-e-apoia-greve-dos-caminhoneiros/>. Acesso em: 10 jun. 2018.

AMARAL, Rodrigo. **"Brasil é quarto em ranking de danos causados por cibercrimes"**. Risco Brasil Seguro (site). Disponível em: <http://riscosegurobrasil.com/materia/brasil-e-quarto-em-ranking-de-danos-causados-por-cibercrime/>. Acesso em: 18 mai. 2018.

AZEVEDO, Marcelo André de; SALIM, Alexandre**. Direito Penal**: Parte Especial. 7. ed. Salvador: Editora Juspodivm, 2018.

BARROS, Laura. **O Hacktivismo no Desenvolvimento da Internet.** Anonymous Brasil (site). Disponível em: <http://www.anonymousbrasil.com/coluna/o-hacktivismo-no-desenvolvimento-da-internet/>. Acesso em: abr. 2018.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. **Comentários à Constituição do Brasil**. v. 2. São Paulo: Saraiva, 1989.

BECK, Ulrich**. Sociedade de risco**: rumo a uma outra modernidade. São Paulo: Editora 34, 2010.

BERETTA, Pedro. "**Sem meios eficazes, Lei Carolina Dieckmann até atrapalha"**. Revista do Consultor Jurídico (online). Disponível em: <https://www.conjur.com.br/2014-mai-10/pedro-beretta-meios-eficazes-lei-carolina-dieckmann-atrapalha>. Acesso em: mai. 2018.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal**. Planalto: portal de legislação. Rio de Janeiro, 31 dez. 1940. Disponível em: <.http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>.

_____. Constituição (1988). Constituição da República Federativa do Brasil: promulgada em 5 de outubro de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: jun. 2018.

_____. Supremo Tribunal de Justiça. Conflito de Competência nº 145.576 - MA (2016/0055604-1). Suscitante: Juízo de Direito da 1ª Vara Criminal de Imperatriz - MA. Suscitado: Juízo de Direito da 1ª Vara Criminal de Bat. Relator: Ministro Joel Ilan Paciornik. Brasília, 20 de abril de 2016.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003.

CHIOVENDA, Giuseppe; ATHENIENSE, Alexandre. **A Jurisdição no Ciberespaço**. Revista Jurídica do CEJ (Centro de Estudos Judiciários). Brasília: Conselho da Justiça Federal, ano 7, nº 20, p. 75, 2003.

COSTA JÚNIOR, Dijosete Veríssimo da. **Jurisdição contenciosa e jurisdição voluntária**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 13, 18 maio 1997. Disponível em: <https://jus.com.br/artigos/776>. Acesso em: jun. 2018.

COSTA, Marco Aurélio. **Crimes de Informática III**. Retirado da Internet. Urugauiana, 1989.

CRESPO, Marcelo Xavier de Freitas. **"As diversas terminologias do universo hacker"**. Canal Ciências Criminais. Set. 2015. Disponível em: <https://canalcienciascriminais.com.br/as-diversas-terminologias-do-universo-hacker/>. Acesso em: 10 jun. 2018.

_____. **Crimes digitais**. São Paulo: Saraiva, 2011.

_____. **“As Leis nº 12.735/2012 e nº 12.737/2012 e os crimes digitais:** acertos e equívocos legislativos”. Canal Ciências Criminais. Disponível em: < https://canalcienciascriminais.com.br/as-leis-no-12-7352012-e-12-7372012-e-os-crimes-digitais-acertos-e-equivocos-legislativos/>. Acesso em: jun. 2018.

_____. **“Sobre os sites que divulgam dados pessoais: uma análise sob a perspectiva criminal”**. Canal Ciências Criminais. Disponível em: <https://canalcienciascriminais.com.br/sobre-os-sites-que-divulgam-dados-pessoais-uma-analise-sob-a-perspectiva-criminal/>. Acesso em: jun. 2018.

CUNHA, Rogerio Sanches. **Manual de Direito Penal:** Parte Especial. 9. ed. Salvador: Editora Juspodivm, 2017.

GARCIA, Gabriel. **“Os 15 hackers que fizeram os maiores estragos da história”.** Revista Exame (online). Disponível em: <https://exame.abril.com.br/tecnologia/os-15-hackers-mais-perigosos-de-todos-os-tempos/>. Acesso em: 05 mai. 2018.

GOETHALS, Karen; AGUIAR, Antónia; ALMEIDA, Eugénia. **História da Internet**, 2000. f Dissertação (mestrado) - Curso de Mestrado em Gestão da Informação, Faculdade de Engenharia da Universidade do Porto, Porto, 2000.

GRECO, Rogério. **Curso de Direito Penal:** Parte Geral. v. 1. 16. ed. Rio de Janeiro: Impetus, 2014.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na Internet**. 2. ed. São Paulo: Juarez de Oliveira, 2009.

KURTZ, João. **“O que é phishing?”**. Techtudo (site). Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/01/o-que-e-phishing-e-malware.html>. Acesso em: jun. 2018.

LICKS, Otto Banho; JUNIOR, João Marcelo de Araújo. **Aspectos penais dos crimes de informática no Brasil**. *In*: Revista dos tribunais Rio Grande do Sul, 1994.

MASSON, Cleber. **Direito Penal:** Parte Geral. v. 1. 12. ed. São Paulo: Método, 2018.

MATSUURA, Sérgio; JANSEN, Thiago. **"Onda de crimes praticados por hackers cresceu 197% no Brasil em um ano".** O Globo**.** Disponível em: <https://oglobo.globo.com/sociedade/tecnologia/onda-de-crimes-praticados-por-hackers-cresceu-197-no-brasil-em-um-ano-17197361#ixzz5JlOe8bth >. Acesso em: 12 jun. 2018.

PLANTULLO, Vicente Lentini. **Estelionato Eletrônico**. Curitiba: Juruá, 2003.

REVISTA CONSULTOR JURÍDICO. **"STJ divulga jurisprudência sobre conceitos de crimes pela internet"**. Disponível em: <https://www.conjur.com.br/2018-jun-17/stj-divulga-jurisprudencia-conceitos-crimes-internet>. Acesso em: 20 jun. 2018.

RIBAS JUNIOR, Douglas. **Lei Carolina Dieckmann e o sistema penal brasileiro.** Canaltech (site). Disponível em: < https://canaltech.com.br/juridico/Lei-Carolina-Dieckmann-e-o-sistema-penal-brasileiro/>. Acesso em: mai. 2018.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo.** 11. ed. São Paulo: Malheiros, 1996.

SILVA, Mauro Marcelo de Lima. **Crimes de informática.** 15. ed. São Paulo: Saraiva, 1997.

_____. **Os crimes digitais hoje**, 2000. Revista do Consultor Jurídico (online). Disponível em: <http://www.conjur.com.br/2000-set-02/policia_revela_perfil_criminoso_internet>. Acesso em: mai. 2018.

SILVA, Rafael. **"Gasto com crimes virtuais no Brasil em 2010 foi de US$ 15 bilhões, diz Symantec"**. Disponível em: <https://tecnoblog.net/77490/symatec-crimes-virtuais-2011/>. Acesso em: jun. 2018.

SOUZA, Artur de Brito Gueiros; JAPIASSÚ, Carlos Eduardo Adriano. **Curso de Direito Penal**. v. 1. Campus Jurídico, 2012.

TANGERINO, Dayane Fanti. “Criminalidade e as novas tecnologias da informação e comunicação”. **Canal Ciências Criminais**. Jan. 2016. Disponível em: < https://canalcienciascriminais.com.br/criminalidade-e-as-novas-tecnologias-da-informacao-e-comunicacao/>. Acesso em: mar. 2018.

_____. “Direito Penal e Novas Tecnologias”. **Canal Ciências Criminais**. Jan. 2016. Disponível em: <https://canalcienciascriminais.com.br/direito-penal-e-novas-tecnologias/>. Acesso em: mar. 2018.

VIANNA, Túlio Lima. **Do rastreamento eletrônico como alternativa à pena de prisão.** *In*: Revista da Ordem dos Advogados (A. 68, t. 2-3, set /dez. 2008).