CENTRO UNIVERSITÁRIO SÃO JOSÉ
CURSO DE DIREITO

FLÁVIA MOREIRA ROSA MORANDI

ANDERSON DE OLIVEIRA AGUIAR

PROF. SOLANO ANTONIUS DE SOUSA SANTOS

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

Rio de Janeiro

2019

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS
THE EVOLUTION OF CYBER CRIMES

FLÁVIA MOREIRA ROSA MORANDI
ANDERSON DE OLIVEIRA AGUIAR
Graduando do Curso de Direito pelo Centro Universitário São José

SOLANO ANTONIUS DE SOUSA SANTOS
Mestre em Direito e Professor da UniSãoJosé

RESUMO

O presente artigo tem como objetivo fazer uma análise quanto ao avanço da tecnologia e a defasagem das Leis que não acompanham essa evolução com a mesma rapidez e devido ao grau de complexidade para que ambos fossem evoluindo em paralelo tendo assim que se adaptar da forma que é possível para coibir a prática de crimes cibernéticos e não ficarem impunes.
Palavras-chave: ação penal,lei 12.737/2012, e 12.965/2014.

ABSTRACT

This article analysis the advancement of technology and the failure in the laws that don`t follow this evolution as quickly as the complexity of this subject, that both were evolving in grow up together. That`s why the law have to adapt as it`s possible to forbid the practice of Cyber Crimes and not let your offenders stay unpunished.
Key-words: criminal action, law 12.737/2012, law 12.965/2014.

INTRODUÇÃO:

Com a evolução da tecnologia, a internet, nos traz uma comunicação em tempo real e para qualquer lugar do planeta que esteja conectado e sendo assim, em se tratando do uso, surgem o que a utilizam para o bem como também os que dela se utilizam para cometer ilícitos.

As Leis não se atualizam da mesma forma como a evolução tecnológica e temos de adaptar para não deixar que os atos ilícitos fiquem impunes, criando algumas Leis, não na quantidade devida ainda, mas na medida em questão criadas vão coibindo os crimes que estão mais recentes e em números expressivos. E como importante processo de identificar esses ilícitos existem órgãos que estão se especializando nesse assunto.

Como exemplo de criação de Leis que não são criadas de forma tão expressiva quanto a tecnologia temos, após 15 (quinze) anos as Leis que foram promulgadas como a de nº 12.737/2012, popularmente conhecida Carolina Dieckmann e a nº 12.965/2014 denominada Marco Civil da internet.

Iremos apresentar como os legisladores procuram agir mediante os crimes cibernéticos e como exemplo de outros países já possuem forte respaldo com relação ao tema.

Embora tenha sido de grande esforço a adaptação da legislação brasileira para coibir a prática de crimes cibernéticos, possuímos uma Lei singular, que não tratam especificamente de crimes da internet.

FUNDAMENTAÇÃO TEÓRICA

Os crimes cibernéticos no mundo tiveram a sua visibilidade a partir da década de 0, que teve como colaborador o matemático John Von Neumann, onde ocorreram as primeiras aparições, bem como a força da globalização que proporcionou grandes modificações na sociedade contemporânea, tendo esse processo iniciado na metade do século XX.

Com o passar do tempo, em 1970 surgiu a expressão *hacker,* 1978 na Universidade de Oxford, nos Estados Unidos, um estudante copiou a prova, ou seja, houve a invasão em seguida a cópia, porém nesta época não existia lei no país que amparasse a instituição com relação ao fato, tendo sido o Estado da Flórida o primeiro a dar o primeiro passo para a criação de leis que versam a informática.

O primeiro hacker a ser condenado efetivamente foi um norte americano, na década de 90 por invadir uma rede de telefonia e provedores da internet nos Estados Unidos, onde ficou preso durante 5 anos, com isso a atividade foi aumentada e na mesma época surgiram outros casos emblemáticos. Já no Brasil, o primeiro crime cibernético ocorreu através da pescaria de senhas em 1999[1]

No Brasil adota o princípio da legalidade e o da reserva legal, onde estabelece que não há crime sem que a lei anterior o defina, porém, quando se trata de crimes da informática. O princípio da legalidade tem previsão expressa na carta magna em seu art. 5°, XL da Constituição federal, que diz: “XL - a lei penal não retroagirá, salvo para beneficiar o réu”

Sendo assim, no país os crimes cibernéticos têm abrangência tanto no Direito Civil, quanto no Direito Penal.

No Direito Civil, a lei n. 12.965/2014, conhecida como “Marco Civil da Internet” que tem como objetivo regular o uso da internet no Brasil, seu projeto de lei foi apresentado ao Poder executivo à Câmara dos Deputados em 2007 que desde então vinha sendo discutido, através da PLC (projeto de lei da câmara) de 21 de abril de 2014 que houve a sua aprovação no Senado[2].

1 Disponível em http://www1.folha.uol.com.br/fsj/cotidian/ff05089912.htm
2 PLC - PROJETO DE LEI DA CÂMARA, Nº 21 de 2014 – Senado

Na esfera Penal, temos a criação da lei de nº 12.735/2012, de 30 de novembro de 2012 foi criada para tipificar as condutas ilícitas que são realizadas nos sistemas eletrônicos, os dados apontados são de 95%[3] de casos que a legislação penal utiliza para coibir e combater os crimes cibernéticos.

Em 2012, quando a artista Carolina Dieckmann[4] teve subtraídas 36 fotos intimas e logo após divulgadas por 5 (cinco) indivíduos que foram identificados e punidos pelos crimes de difamação, extorsão e furto, porém no que tange a invasão do computador, ambos não foram punidos.

Devido a esse caso, foi criada a lei 12.737/2012 sancionada pela presidente Dilma Rousseff, esta lei teve a sua tramitação em regime de urgência no Congresso Nacional, com isso houve alteração no código penal, a inclusão do art. 154-A do CP, conhecida como intrusão informática:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. (Incluído pela Lei nº 12.737, de 2012) Vigência
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência

---

3 ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal.* São Paulo: Memória Jurídica, 2004.
4 Disponível em: https://www.metrojornal.com.br/entretenimento/2018/01/08/carolina-dieckmann-diz-que-fotos-vazadas-viraram-lembranca-boa.html

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência Ação penal (Incluído pela Lei nº 12.737, de 2012) Vigência”

A ação penal dos crimes cibernéticos, em regra, será pública condicionada à representação, salvo nos casos previstos no art. 154-B do Código penal, ou seja, o delito pode é crime comum que pode ser cometido por qualquer pessoa, já a vítima pode ser qualquer pessoa, sendo ela física ou jurídica.

A sua consumação dar-se-á no ato da invasão ao dispositivo informático do indivíduo alheio, podendo estar conectado ou não à rede de computadores e com isso infringir sua segurança.Essa prática de atividade ilícita tem como finalidade obter, alterar ou destruir dados, informações, com o intuito de obter vantagem indevida.

Sua pena é de detenção, de 3 (três) meses a 1 (um) na, e multa, podendo ser aumentado de acordo com os parágrafos do referido artigo para reclusão, de 6 (seis) meses a 2 (dois) anos, e multas, dependo da conduta do agente causador. Se assim, trata-se de infração penal de menor potencial ofensivo, ou seja, abrange a lei 9.099/1995 dos juizados especiais criminais.

Todavia, a competência para processar e julgar crimes desta natureza será a Justiça Estadual, pois a prática deste crime não está previsto em tratado ou convenção internacional em que o Brasil se comprometeu a conflitar, ao contrário do que ocorre com os crimes de xenofobia, racismo, dentre outros[5].

Já o art. 154-B do Código Penal Brasileiro, que também adveio da lei 12.737/2012, tem como objetivo a punição ao agente que comete ato ilícito contra a administração pública direta ou indireta, sendo qualquer ente federativo:

> "Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012) Vigência"

Em regra, a ação penal será pública condicionada à representação do ofendido ou de quem for o seu representante, pois se subentende que uma eventual exposição poderá causar constrangimento a vítima, sendo assim ficará a critério da vítima ou do seu representante a autorização do início da persecução penal.

Diferentemente, será ação penal pública incondicionado, nos casos em quem tenha sido o lesado a administração pública, pois há ofensa ao bem jurídico nesses casos é de natureza indisponível.

5 Ferreira, Aurélio Buarque de Holanda, Mini Aurélio: o dicionário da língua portuguesa/Aurélio Buarque de Holanda Ferreira; coordenação de edição Marina Baird Ferreira. – 8. Ed. – Curitiba: Positivo, 2010.

Com base na leitura, concluímos que o estopim para que os deputados criassem um projeto de lei, adveio das fotos vazadas nas redes sociais, no mundo do digital da atriz Carolina Dieckmann.

Sabemos que a prática deste delito é antiga, desde o século XX, tendo como pioneiro os Estados Unidos. No Brasil, o primeiro político a sofrer com esses ataques foi o ex-Prefeito Paulo Maluf, no ano de 2000, sendo o crime de sabotagem digital nas eleições.

EVOLUÇÃO HISTÓTICA DOS CRIMES CIBERNÉTICOS

Os crimes cibernéticos tiveram início no ano de 1960, onde foram registradas alterações de cópias e sabotagens de sistemas. Após o colapso desta infração, surgiu a propagação de vírus, pornografia infantil, pirataria e a invasão de sistema.

Já na década de 70, houve a citação de *hacker,* segundo Aurélio Buarque de Holanda Ferreira[5], podemos definir esse termo como: “Indivíduo perito em informática que invade, em geral, ilegalmente, sistemas de computadores.”

A partir da década de 90, tivemos como personagens Robert Morris, que ficou conhecido como o primeiro *hacker* no mundo cibernético, onde foi o causador da propagação do primeiro vírus, onde afetou cerca de 6 (seis) mil computadores, Kevin Mitnick, norte-americano, adentrou em provedores de internet americano e em redes de computadores de operadores telefônicas, devido a isso foi preso em 1995, onde ficou detido durante 5 (cinco) anos e Kevin Poulsen interceptou uma ligação telefônica de uma emissora de rádio no Estado da Califórnia que estava realizando um sorteio, onde o 102º ouvinte, ganharia um carro da marca Porsche, devido essa façanha ficou preso durante 4 (quatro) anos e hoje é diretor do *site* Security Focus.

No Brasil há registros de que os primeiros crimes iniciaram na década de 90, conhecido pescaria de senhas ou crime de *phishing scam,* ou seja, era uma técnica fraudulenta utilizada por criminosos para subtraírem senhas de banco, bem como informações pessoais.

O ex-Prefeito de São Paulo, Paulo Maluf, foi o primeiro político brasileiro que foi vítima de crime cibernético, onde, no ano de 2000, houve sabotagem digital nas eleições, porém, a primeira condenação no país ocorreu apenas em 2004, onde um jovem foi responsabilizado por aplicar golpes no Brasil e nos Estados Unidos, usando como ferramenta a internet, tendo sido condenado em 6 (seis) anos e 4(quatro) meses.

CARACTERÍSTICAS DAS CONDUTAS DOS CRIMES CIBERNÉTICOS

Podemos destacar algumas condutas que são caracterizadas como crime cibernéticos:

1. **Acesso ilegítimo:** é quando o indivíduo entra sem autorização nos sistemas, porém não é caracterizado como violação de segurança. Com relação a legislação vigente há divergências doutrinária, pois para alguns doutrinadores o acesso ilegítimo, no século XXI, está caracterizado no tipo penal com a lei de n. 12.737/2012. Já para a outra parte da doutrina, diz que no país este tipo penal está previsto no art. 154-A do Código Penal, porém apenas para os casos de invasão.

2. **Interferência de dados:** é praticado por um ou mais indivíduos e tem como objetivo apagar, deteriorar, alterar ou eliminar dados, ou seja, caracteriza-se um dano a informática. Este crime está previsto no art. 154-B do Código Penal e na lei de n. 12.738/2012. Agora se o agente não pratica a invasão, somente o dano informático, será regido pelo art. 163 do Código Penal que trata de crimes de danos.

3. **Interferência em sistemas:** está correlacionada com a conduta dos agentes que agem com dolo e tem como escopo final causar grave obstrução, quando teve a intenção de causar e com isso o resultado foi a danificação, eliminação e deterioração dos dados informáticos. Verifica-se que a legislação brasileira não comporta todos as condutas acima citadas, com a criação da lei de n. 12.737/2012, houve a tipificação da conduta com relação a interrupção e turbação dos serviços telefônicos, informáticos e telemáticos.

4. **Falsidade ou fraude informática:** é quando o agente introduz, altera ou elimina dados informáticos verdadeiros e são substituídos por dados não autênticos, com o objetivo de que estes sejam utilizados como se fossem verídicos, porém não há legislação específica para esta conduta.
   Insta salientar que esse tipo de crime poderá ser praticado por funcionário público contra administração pública e a punição está prevista no art. 313-A do Código Penal.

5. **Burla informática:** ou mais conhecida como sabotagem informática, sendo este um ato intencional onde o agente introduz, elimina ou anula os dados informáticos, tendo como finalidade o benefício econômico destes atos.

O POSICIONAMENTO DOS PAÍSES DA AMÉRICA DO SUL

Percebe-se que no Peru, país que compõe América do Sul, a conduta punitiva deu-se através do Decreto Legislativo de n° 635, onde buscou punir delitos como o acesso e uso indevido de bancos de dados, sistemas computacionais ou rede.

O Código Penal peruano foi promulgado em 3 de abril de 1991 e publicado em 8 de abril do referido ano, porém o projeto de lei que trata os crimes cibernéticos só foi promulgado em 12 de setembro de 2013, onde a lei tipificou delitos como violação de intimidade, delito de furto, tendo como agravante a transferência eletrônica, emprego de senhas secretas e delito de fraude da administração de pessoas jurídicas na

modalidade de uso de bens informáticos, porém o mencionado texto foi bastante questionado por parlamentes, pois a sua aprovação ocorrera de forma clandestina e houve violações aos princípios do direito penal.

Já o Chile, tem a sua própria legislação que versa sobre o crime informático, sendo este a lei 19.223 que foi publicada em 7 de junho de 1993 e tem como pretensão a punibilidade da destruição de dados, dentre outras condutas.

Insta mencionar que o país é um dos primeiros na América do Sul a atualizar a sua legislação, conforme o avanço dos crimes cibernéticos.

Na Argentina, a legislação que tipifica a conduta do agente está prevista da Lei de Proteção de Dados que pune o uso indevido destes cedidos por titulares, bem como o acesso não autorizado. Já o Código Penal argentino, sofreu alterações em 2008, onde foi incluído os chamados crimes digitais.

Nota-se que no Brasil a sua legislação não acompanhou o avanço significativo dos crimes cibernético, sendo o seu Código Penal é de 1940, ou seja, antes da criação das leis 12.735/2012 e 12.737/2012, onde foi realizada a inclusão dos arts. 154-A e 154-B no Código Penal brasileiro, pois a legislação era vaga e escassa.

CRIAÇÃO DAS LEIS 12.735/2012 E 12.737/2012

1. **LEI 12.735/2012:** prevê a tipificação da conduta delituosa do uso de sistema eletrônico contra sistemas informatizados e militares. O seu projeto de lei n°84/99 alterou o Código Penal brasileiro e o Código Penal Militar.
   O art. 4º da lei 12.735-2012, trata da polícia judiciária com o intuito de constituir combate as ações delituosas em redes, sistemas informatizados, bem como dispositivos de comunicação.

Sucede que, a referida lei teve dois vetos em seu texto final, em seus artigos 2° e 3°, ambos feitos pelo Presidente da República, onde foi encaminhado para o Congresso Nacional.

O projeto de lei n°84/99 tramitou no Congresso durante 12 (doze) anos, onde previa diversos tipos penais, dentre eles a pornografia infantil que estava no art. 20, onde teria penas mais severas para a prática deste delito, porém quando estava em trâmite houve alteração na legislação do Estatuto da Criança e do Adolescente, onde versou sobre o tema.

O projeto previa em seu art. 21 que a competência para processar e julgar a prática do crime de pornografia seria no âmbito Federal, no entanto quebraria o pacto federativo que traz a Constituição da República Federativa do Brasil de 1988, onde todas as demandas seriam tratadas na Justiça Federal e Polícia Federal.

2. **Lei 12.737/2012:** ficou conhecida no país como “Lei Carolina Dieckmann”, onde tratou como crimes cibernéticos e originou o projeto de lei n°2.793/2011, onde apressou a publicação da lei n°12.737/2012.
   A lei 12.737/2012 trouxe alguns tipos penais, conforme demonstrados a seguir:

   - Invasão de dispositivo informático: que seria a cópia de dados ou informação, onde ocorria antes da lei, sendo as denuncias tipificadas com base no art. 155 do Código Penal que trata sobre os crimes de furto. Com a vinda da lei 12.737/2012, o Código Penal teve alteração em seus artigos e hoje a prática do deste delito é previsto no art. 154-A do Código Penal.
   É classificado como crime instantâneo, tendo em vista que a sua consumação ocorre no ato da invasão. Essa prática pode ser feita por qualquer pessoa, sendo admitida a modalidade culposa. A sua consumação é comprovada através de prova pericial, onde um perito especializado, responde os seguintes questionamentos: a data e hora do login e a data e hora da finalização do logout,

dentre outros quesitos. A tentativa irá ocorrer mediante a um ataque de força bruto a um firewall, conhecido como porta corta fogo.

A ação penal será pública condicionada à representação, onde a pena será inferior à 2 (dois) anos, sendo o juízo competente para processar e julgar esta demanda o Juizado Especial Criminal.

-Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública: Esta modalidade de crime seria a interrupção doce serviço de tecnologia dar informação, Sendo o seu principal meio de agir através de um ataque de negociação de serviços, o que é a tentativa de tornar os recursos de sistemas como a web, por ser mais vulnerável a realização da invasão.

Destaca-se que o artigo 266 do Código Penal, previa a prática de interrupção ou perturbação dos serviços telegráficos, radiotelegráficos ou telefônicos, tendo como pena de detenção de 1 (um) a 3 (três) anos.

Com a lei 12.737/2018, acrescentou o parágrafo 1° na referida lei, que diz:

> “Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.”

Este crime pode ser cometido por qualquer pessoa e o sujeito lesado será o Estado. A consumação do delito irá ocorrer de acordo com o caput do art. 266 do Código Penal e precisa ser comprovado mediante laudo pericial. A ação penal será pública incondicionada, sendo a competência o juízo comum.

Nesse caso, não caberá o Juizado Especial Criminal por se tratar da necessidade da produção de provas como a realização da perícía e conforme a lei 9.099/1995, não é cabível esse meio de provas.

Falsificação de documento particular: já era prevista a prática de crime em nosso ordenamento jurídico, de acordo com o art. 298 do Código Penal. Ocorre que com a lei 12.737/2012, inseriu o parágrafo único onde iguala os documentos particulares aos cartões de débito e crédito, que diz:

> "Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
> Pena - reclusão, de um a cinco anos, e multa.
> Falsificação de cartão(Incluído pela Lei nº 12.737, de 2012) Vigência
> Parágrafo único. "Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito."

Trata-se de crime instantâneo, onde consumado se encerraria e necessitaria do exame de corpo de delito quando tratar de crime permanente. Já quando o agente falsifica o cartão de débito e crédito, será crime comissivo.

O sujeito ativo será qualquer pessoa e o lesado será o Estado ou pessoa natural. Ocorrerá a consumação a partir da falsificação ou alteração do documento e a ação penal prevista nesses casos será a pública incondicionada.

CRIMES CIBERNÉTICOS: A UTILIZAÇÃO DO BIG DATA E DO BIG DATA E DO DETECTA PARA A PREVENÇÃO DE CRIMES

Ao longo do tempo a humanidade foi se adaptando as novas tecnologias quando ocorreu o advento da era digital e o surgimento do chamado "ambiente digital", dando assim amplo acesso e bastante diversificado para todas as pessoas, entretanto com a utilização com finalidade lícita assim como os que de forma ilícita com práticas que devem ser objeto de punição.

Como uns dos atos ilícitos podem citar as *fake news*, um fato grave, que tem um impacto direto na vida social tanto na vítima como em seus familiares. Sendo essa prática no ambiente online onde se ocorre violações de segurança, intimidade, “pornografia infantil”, assédio, bullying e até mesmo exploração sexual infanto-juvenil.

Por estarmos conectados em rede a celeridade e interação social ocasionou muitas mudanças quanto a comunicação assim como o rompimento de barreiras, antes mais físicas para agora o meio digital.

Os termos usados para destacar como “Cibercrime[6]”, “Crimes Cibernéticos”, “Crimes Digitais”, dentre outros são para ter uma identificação dos diferentes delitos praticados no “mundo” virtual da internet, e como umas das condutas que podemos destacar de acesso não autorizado informatizado temos a interceptação de comunicações modificação de dados, incitação ao ódio e outras como condutas delituosas.

No território brasileiro como destaque temos o crime digital, por exemplo, assim determinado por meio da aprovação da Lei 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann que modifica o código penal e tipifica condutas no ambiente virtual, tanto como invasão de computadores assim como levou ao estabelecimento de punições específicas. Essa lei alterou a redação dos artigos 266 e 298 do Código Penal adequando-a para realidade cibernética. As punições são possíveis de ser aplicadas a provedores de internet para que estes apaguem o conteúdo assim como se tem julgado pelo STF nesse sentido.

O artigo 266 teve sua titulação alterada no caminho de inserção da idéia de interrupção relativos aos serviços de informática abordando o seguinte delito “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”.

6 –COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na área da informática HTTPS://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica , Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 7 Acesso em:13 abril 2018.

Quanto ao artigo 298, em seu parágrafo único, o legislador buscou equipar como documento particular os cartões de crédito no delito de falsificação de documento.

Com sendo crime, a lei classifica justamente situações semelhantes, em que ocorre a configuração de invasão de computadores, tablets ou smartphones, conectados ou não à internet, “com o fim de obter, adulterar ou destruir dados ou informações”.

Sobre as diferentes formas e espécies de cometimento de um crime cibernético, Colares[6] nos ensina que:

> Crime conta a segurança nacional, preconceito, discriminação de raça-cor e etnias, pedofilia, crime contra a propriedade industrial , interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software, calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação de direito autoral, escárnio por motivo de religião, favorecimento de prostituição, ato obsceno, incitação ao crime, apologia ao crime ou criminoso, falsa identidade, inserção de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões e jogo de azar (2002, p 02)

Os usuários estão conectados ao ambiente virtual, o que permite desenvolver interatividade com outros usuários, de maneira a possibilitar uma série de atividades, relacionadas ao campo profissional, pessoal, entretenimento entre outros, nas quais como qualquer atividade pode ser utilizada para realização de ações maléficas.

Inúmeros delitos considerados como fraudes, invasões a sistemas particulares dentre outras condutas que afetam consideravelmente o universo virtual, de agora em diante há necessidade do Direito Penal ter que evoluir no sentido de criminalizar tais condutas, pois são de fatos Crimes Cibernéticos.

Como necessidade de prevenção e de combate aos crimes virtuais é necessário o desenvolvimento e utilização de novas tecnologias que surtam efeitos desejados em tal combate.

Com a necessidade de surgir um aumento de capacidade de gerar, armazenar, coletar e tratar dados surgiu o Big Data, sendo um termo que se descreve a geração de impactos nos negócios do dia a dia, sendo utilizado por inúmeras empresas para analisarem comportamentos sociais comuns e promoverem com isso uma campanha de melhoria nas suas estratégias, abrangendo, portanto, técnicas de cruzamento e tratamento de dados com o objetivo de levar a extração de conclusões para afinar novos resultados.

Com capacidade de identificar uma série de comportamentos e tendências sociais, o Big Data, não vem a serem somente utilizados como melhoria de serviços, produtos, etc. A utilização do Big Data para fins criminais é de extrema importância, tendo em vista que ajudaria consideravelmente para que sejam desenvolvida estratégias de prevenção de crimes.

Utilizado nos Estados Unidos desde 2011, o Big Data, em meio a ações que visam a prevenção de crimes diversos, permitindo assim atuação em caráter antecipado da ação da Polícia e que possam levar até a captura de potenciais criminosos antes de cometerem novos crimes.

A Prefeitura de São Paulo adquiriu o sistema DETECTA, o qual foi desenvolvido pela Microsoft juntamente com a prefeitura de Nova York, assim, o sistema possui a funcionalidade de executar um processo de monitoramento criminal, com o intuito de analisar os dados obtidos pelo INFOCRIM e pelo Registro Digital de Ocorrências, no qual trabalha diretamente no sistema de prevenção criminal, em situação análoga ao sistema de Big Data, o que contribuem auxiliar as investigações desenvolvidas pela Polícia.

O Big Data (conjunto de informações armazenadas) sendo o maior sistema de monitoramento inteligente da América Latina, que integra banco de dados das polícias paulistas, como os registros de ocorrências, Fotocrim (banco de dados de criminosos com arquivos fotográficos), cadastro de pessoas procuradas e desaparecidas, dados do Detran (Departamento Estadual de Trânsito), registro de veículos furtados, roubados, clonados e outros relatórios inteligentes de segurança pública.

CONSIDERAÇÕES FINAIS

Vimos que com o avanço da internet a população ficou vulnerável aos ataques cibernéticos, pois qualquer indivíduo tem acesso a rede informática independente da sua localização. Devido a isso, foram surgindo diversos atos ilícitos como: inserção de dados falsos, invasão aos servidores, dentre outras práticas, que ocorreu pelo mundo no século XX.

Com o crescimento desenfreado dos ataques, a legislação vigente a época mostrou-se despreparada e desamparada para punir estes delitos, sendo necessário que houvesse atualizações em sua norma jurídica. No Brasil, essa atualização ocorreu apenas no século XXI, quando a atriz Carolina Dieckmann teve suas fotos intimas subtraída de seu notebook e logo após divulgadas na internet. A partir desse momento foi promulgada a lei 12.737/2012, onde sua tramitação foi considerada pelo Congresso Nacional como urgente. Sendo que, antes da prática do referido delito, não havia uma lei específica que punisse os infratores, e após a vigência da lei considera-se como crime consumado a prática de invasão ao dispositivo informático individual alheio, ou seja, qualquer aparelho tecnológico sem distinção.

Após o sancionamento da lei 12.737/2012 o código penal brasileiro sofreu alteração, com a inclusão dos artigos. 154-A e 154-B, que versam sobre o caso em tela e busca punir o ato ilícito do agente que invade o dispositivo alheio e os crimes praticados contra a administração pública direta ou indireta. Já a lei 12.735/2012,

alterou o Código Penal Militar e o Código Penal Brasileiro, pois essa legislação prevê crimes contra o sistema informatizados e militares.

Nota-se que as características das condutas dos crimes cibernéticos são conduta realizadas pelo agente, onde ele acessa, interfere, frauda, falsifica, burla e que podem ser praticado por qualquer indivíduo, não sendo considerado crime próprio, ou seja, não é necessário ser cometido por um agente específico.

Diversos países da América do Sul, como Peru, Chile, Argentina, já se posicionaram sobre a matéria e tem amparo legislativo para determinada prática ilícita. Podemos citar como pioneiro dessa mudança o Chile que, ao notar o grande avanço da tecnologia, foi um dos primeiros países a atualizar a sua legislação para receber o novo delito.

Então, a criação das legislações citadas acima, veio para que a legislação acompanhasse a evolução histórica da internet, o seu crescimento, punir os agentes que utilizam desta ferramenta para praticar ato ilícito prejudicial a outrem.

REFERÊNCIAS:

Mulheres da advocacia criminal: temas atuais de direito e processo penal
Organizadora Wanessa Fernandes Ribeiro - 1.ed - Florianópolis: Tirant lo Blanch, 2019. 225p.
1.Violência contra mulher. 2. Direito penal das mulheres. 3. Compliance officer. 4. Feminicídio no Brasil. I. Título.

MASSON, Cleber, 1976
Código Penal comentado / Cleber Masson. 3. ed. rev., atual., e ampl. - Rio de Janeiro: Forense; São Paulo; MÉTODO, 2015.
1. Direito Penal - Brasil. 2 Processo penal - Brasil 3. Direito penal I. Título.

JESUS, Damásio de

Manual de crimes informáticos / Damásiode Jesus, José Antonio Milagre. - São Paulo: Saraiva, 2016.

GRECO, Rogério.

Curso de Direito Penal / Rogério Greco. - 17. ed. Rio de Janeiro: Impetus, 2015.