UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO

FLOR VIOLETA SOARES GUIMARÃES

CRIMES CIBERNÉTICOS: UMA ANÁLISE CRÍTICA, ATUAL E CONTEXTUALIZADA À LUZ DA INVASÃO DE PRIVACIDADE

JUIZ DE FORA
2019

FLOR VIOLETA SOARES GUIMARÃES

CRIMES CIBERNÉTICOS: UMA ANÁLISE CRÍTICA, ATUAL E CONTEXTUALIZADA À LUZ DA INVASÃO DE PRIVACIDADE

Trabalho apresentado à Disciplina de MONOGRAFIA DE CONCLUSÃO DO CURSO DE DIREITO, como parte dos requisitos para obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Luiz Antônio Barroso Rodrigues

Juiz de Fora

2019

FLOR VIOLETA SOARES GUIMARÃES

CRIMES CIBERNÉTICOS: UMA ANÁLISE CRÍTICA, ATUAL E CONTEXTUALIZADA À LUZ DA INVASÃO DE PRIVACIDADE

Trabalho apresentado à Disciplina de MONOGRAFIA DE CONCLUSÃO DO CURSO DE DIREITO, como parte dos requisitos para obtenção do título de Bacharel em Direito.

Aprovada em 17 de Junho de 2019.

BANCA EXAMINADORA:

_____

Prof. Dr. Luiz Antônio Barroso Rodrigues - Orientador
Universidade Federal de Juiz de Fora

_____

Prof. Dr. Cleverson Raymundo Sbarzi Guedes
Universidade Federal de Juiz de Fora

_____

Prof. Dr. Cristiano Alves Valadares do Lago
Universidade Federal de Juiz de Fora

Dedico este trabalho ao meu grande e infinito amor, Eduardo Goulart, por ser a minha inspiração e a minha força de todos os dias. Minha vida, a frase “te amo mais que tudo” tinha que estar presente aqui. Obrigada pelas alegrias e amores infinitos que dividimos quando estamos juntos. Dedico a presente obra também aos meus pais, amores incondicionais, que sempre me apoiaram durante esses cinco longos anos, e a minha vó, que sempre me esperava. Dedico também a minha irmã Flora Guimarães. Você é meu porto seguro, e a reunião de tudo de bom que existe nesse mundo. Obrigada por ter nos dado nosso precioso Henri.

Agradeço ao meu eterno amor Eduardo Goulart, por me apoiar e sempre estar ao meu lado, dando vida ao meu coração, e à Flora Guimarães, minha melhor amiga, irmã e mãe, que me ajuda e sempre me coloca para frente. Amo vocês.

“ A internet é a primeira coisa que a humanidade criou e não entende, a maior experiência de anarquia que jamais tivemos”.

(Eric Schimidt)

RESUMO

Este trabalho possui como objetivo a análise crítica e atual dos crimes cibernéticos, que foram contextualizados, no Brasil e no Mundo, tendo como perspectiva a proteção da privacidade da vítima. Os dispositivos informáticos e suas tecnologias, como a Internet, que inegavelmente fazem parte do cotidiano social, propiciaram uma maior facilidade para a prática de crimes, fazendo-se necessário legislações especiais que tipificassem as novas condutas, como foi o caso da Lei de nº 12.737 de 2012. Lado outro, a experiência no âmbito digital acabou por nos mostrar a eminente indispensabilidade de tipificar práticas que não seriam próprias da informática, mas que utilizavam como principal meio de execução as tecnologias, principalmente a internet. Por tal motivo, considera-se que os novos Arts. 216-B e 218-C do Código Penal podem ser caracterizados como crimes cibernéticos, pelo meio de execução adotado em suas condutas.

Palavras-chave: 1.Crime. 2. Cibernético. 3. Privacidade. 4.Invasão. 5.Meio de execução.

ABSTRACT

This work has as objective the critical and current analysis of cyber crimes, which were contextualized, in Brazil and in the World, with the perspective of protecting the privacy of the victim. Computer devices and their technologies, such as the Internet, which undoubtedly are part of social daily life, have made it easier to commit crimes, requiring special legislation to typify new behaviors, such as Law No. 12.737 of 2012. On the other hand, experience in the digital sphere has shown us the imminent indispensability of typifying practices that would not be typical of computing, but which used as the main means of execution the technologies, especially the internet. For this reason, it is considered that the new Arts. 216-B and 218-C of the Criminal Code can be characterized as cyber crimes by the means of execution adopted in their conduct.

Keywords: 1.Crime. 2. Cybernetic. 3. Privacy. 4. Invasion. 5.Means of execution.

SUMÁRIO

1)INTRODUÇÃO……1
1

2) HISTÓRICO……..…15

2.1) Estatísticas dos cibercrimes no Brasil e no mundo……..……...20

3) DIREITO COMPARADO……..……..24

3.1) Convenção de Budapeste……....…….25

3.2) Direito Penal Informático no Mundo…….……...27

3.2.1) Estados Unidos…….....28

3.2.2) Alemanha……...29

3.2.3) Filipinas……..30

3.2.4) Itália……....31

3.2.5) Índia…….32

3.2.6) Japão……..32

3.2.7) França…….33

3.2.8) Inglaterra……34

3.2.9) Portugal……..35

3.2.10)Espanha……....36

4) DAS FONTES LEGISLATIVAS PENAIS BRASILEIRAS……..37

4.1) Lei nº 12.735 de 2012……37

4.2) Lei nº 12.737 de 2012……40

4.2.1) Análise do tipo penal……....43

4.2.2) Crimes comparados ao de Invasão……...56

4.2.3) Figuras Qualificadas…….57

4.2.4) Causas de Aumento de Pena…….59

4.3) Lei nº 13.772 de 2018 e o novo crime do artigo 216-B do código penal……...60

4.3.1) Análise do Art. 216-B do Código Penal…….61

4.3.2) Porque o delito do Art. 216-B pode ser considerado crime cibernético?.....68

4.4) Lei nº 13.718 de 2018 e o novo crime do Art. 218-C do Código Penal……...……...69

4.4.1) Análise do tipo penal……..……71

4.4.2)Vazamento de imagens íntimas na internet……...……....81

4.4.3) Caso Neymar e sua adequação ao tipo 218-C do Código Penal……...84

5) CONCLUSÕES…….87

6) REFERÊNCIAS BIBLIOGRÁFICAS…….90

1)INTRODUÇÃO

Atualmente, vivemos em uma sociedade fruto da globalização e da evolução diária da tecnologia. A Globalização, dentre seus efeitos, nos proporcionou o progresso cibernético e sua acentuada entrada para o cotidiano social. As distâncias foram “encurtadas”, e as relações interpessoais passaram a se desenvolver através da internet. Pessoas das mais diferentes culturas passaram a se conhecer e a fazer interações por meio da chamada “rede mundial de computadores”, fazendo com que a era digital fosse a responsável pelas novas relações sociais construídas.

Conforme a sociedade passa por evoluções culturais, políticas e tecnológicas, o direito; a seu turno, vai se adaptando às novas necessidades, elaborando novas normas visando a regulação de condutas que eram inimagináveis há alguns anos. O direito verifica, portanto, que a adequação à nova realidade se faz extremamente necessária, caminhando junto com a segurança da informação, fazendo com que a nova sociedade nascida do mundo cibernético não se torne uma sociedade à margem do controle do Estado ou, lado outro, da autotutela.

A ascensão da tecnologia, como a popular e indispensável internet, tem suas implicações e se insere de maneira profunda e essencial no cotidiano das pessoas, elevando a complexidade das relações pessoais e colocando em risco direitos de personalidade do indivíduo, como a privacidade e a intimidade. Nesse sentido, o Art. 21, caput, do Código Civil de 2002:

> “**Art. 21**. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.”

Por esse ângulo, há a proteção conferida pelo Art. 5º, inciso X da Constituição Republicana Federativa Brasileira, de 1988:

> "**Art. 5º** Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> **X** - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. "

Vivemos na chamada "Sociedade do Risco". Em tal sociedade, as pessoas consentem em correr alguns riscos, que se caracterizam como consequências geradas pelas facilidades advindas da tecnologia, porém, alguns riscos devem ser mitigados, como o associado à criminalidade digital. As práticas delituosas agora são cometidas em um novo e pouco explorado ambiente, sendo mais comuns a cada dia, principalmente com a facilidade do instrumento da internet.

Se faz importante colocar em voga, para o melhor entendimento de como o bem jurídico em questão é ameaçado, a explicação dos que seriam os especialistas dos crimes cibernéticos, os chamados "*crackers"* (não diz respeito aos "*hackers"* - estes seriam pesquisadores de segurança da informação), que exploram as intimidades e as minúcias dos sistemas, assim como os processos desenvolvidos sobre a tecnologia da informação, para a prática de delitos. Dessa forma, os cidadãos que não decidem ingressar no mundo cibernético, sendo apenas lançado nesse grande universo digital, se tornam vítimas frágeis e desinformadas.O saber da tecnologia revela aos seus profissionais ou a qualquer indivíduo que conheça a fundo seu funcionamento um imenso poder, trazendo como grande problema o uso deste poder para más finalidades. Vivemos em um País em que a educação digital não é difundida, sendo confundida, por várias vezes, com noções básicas e puramente procedimentais administradas em aulas de informática. Até poucos anos atrás, se discutia se realmente haveria a necessidade da elaboração de uma

legislação especial sobre os crimes informáticos, ou se apenas a simples adequação serviria, necessitando apenas de ligeiras mudanças, muitas vezes confundindo o objeto do crime e o meio da prática do crime.

É certo e incontestável que, pelo princípio da legalidade, não existe crime sem lei anterior que o defina, nem há pena sem sua prévia cominação legal. Ninguém, dessa forma, pode ser responsabilizado por conduta que a lei não considera como de relevância penal. Por isso, frente à necessidade de proteção à esses novos riscos e violações inerentes a sociedade de informação, que estão presentes diariamente em nosso cotidiano, as leis que estabelecem os direitos dos internautas e os consequentes deveres dos prestadores são fundamentais para uma efetiva proteção dos bens jurídicos ameaçados.

Adotando-se, a priori, a legislação criminal (que deveria ser concebida como a *ultima ratio*), o Brasil pune as condutas que são praticadas contra os sistemas informáticos, assim como aquelas que utilizam os mesmos como intermédio. O presente trabalho busca a análise da problemática da proteção da privacidade frente aos crimes cibernéticos, como foram tipificados pelas novas Leis e se realmente são efetivos em tal âmbito. Inescusável é a elucidação do conteúdo das legislações, em qual contexto as mesmas sobrevieram, assim como suas condutas, práticas e técnicas que tipificariam os crimes cometidos na internet e por meio de seus dispositivos informáticos.

Atualmente, com a popularidade da internet e a maior facilidade em ter acesso à informações e à comunicação em massa, já se encontram muitas publicações, artigos e opiniões sobre os crimes cibernéticos no Brasil. Muitas dessas publicações levam em conta o direito alienígena, buscam adaptações no próprio sistema penal vigente ou se baseiam apenas em estatísticas. Porém, no presente trabalho, considero apenas as leis que foram ingressadas recentemente no Ordenamento Jurídico Brasileiro, quais sejam, as leis nº12.735 e nº12.737, ambas

de 2012, e os Arts. 216-B e 218-C, ambos do Código Penal, assim como suas consequências, à luz do contexto da proteção efetiva da privacidade e da intimidade do indivíduo.

Não tendo a pretensão de esgotar o assunto tecendo palavras finais sobre o tema, pretendo fornecer reflexões e dúvidas, para que possamos diferenciar, das infinitas condutas realizadas no terreno cibernético, quais poderão ser enquadradas como crime e, consequentemente, se as novas leis em uso se mostram efetivas ao atender seu mister. Dispõe-se, destarte, um estudo detalhado das leis nº 12.735/2012, nº 12.737/2012 e dos Artigo 216-B e 218-C do Código Penal, apresentando um estudo atualizado e minucioso de seus conteúdos.

Questões como “Quais os principais crimes praticados na internet?’, “Como o ordenamento jurídico pátrio e o de outros Países tratam sobre as práticas criminosas perpetradas na internet?’, “O que já foi feito e o que vem sendo feito em nosso ordenamento jurídico em relação aos crimes Virtuais?” são abrangidas no respectivo trabalho, no sentido de serem respondidas e desenvolvidas.

2) HISTÓRICO

O Brasil ocupa atualmente o 4º lugar no ranking mundial de usuários da internet[1]. Com mais de 120 milhões de usuários, o Brasil sucede apenas os Estados Unidos, que possuem 242 milhões de pessoas conectadas, a Índia, que possui cerca de 333 milhões de internautas e a China, que fica em primeiro com seus 705 milhões de conectados. Os dados pertencem à uma pesquisa realizada pela Conferência das Nações Unidas sobre o Comércio e o Desenvolvimento (UNCTAD, na sigla em inglês)[2]. Já pesquisas realizadas pelo Instituto Brasileiro de Geografia e Estatística, o IBGE, revelam que o equivalente à 64,7% desse total de usuários possuem idade acima de 10 anos, e cerca de 63,3% das casas brasileiras já possuem acesso à internet [3].

Diante dos impressionantes índices brasileiros, não há como negar que a internet se torna cada vez mais popular em nosso País. Cada vez mais incorporado ao cotidiano dos brasileiros, a internet se tornou uma fonte importante e crucial de informações, sendo utilizada em grande escala, inclusive por órgãos públicos. E, como ocorre em todas as etapas do desenvolvimento humano, a criminalidade seguiu e se adaptou à essa nova realidade sociológica.

O Brasil, apesar de ser um dos primeiros países no ranking dos usuários diários do ciberespaço, não foi um dos primeiros a ter que lidar com os crimes informáticos. No mundo, a literatura penal indica que tais crimes tiveram seu início na década de 1960, onde identifica-se as primeiras referências sobre o tema, em sua maioria crimes de cópia, sabotagem e alteração de sistemas computacionais. Já

---

[1]Disponível em: <http://info.abril.com.br/noticias/seguranca/brasil-e-o-4-pais-com--maior-numero-de-ameacas-virtuais-04052012-16>.
[2]Disponível em: <https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/>.
[3]Pesquisa disponível em: <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>.

na década de 1970, já se encontrava menções ao termo “hacker”, e ao termo “sociedade da informação”.

Não é recente, pois, a preocupação com os crimes cometidos no âmbito informático. Desde meados da década de 1960, quando o mundo passa a ter seus primeiros contatos com os crimes cometidos mediante computadores, a sociedade reconhece que é necessário buscar formas de controlar tais condutas nocivas, vindas do avançar tecnológico. Grandes casos ocorridos na época impressionavam as pessoas, e intimidavam os juristas, pois os mesmos, à época, estavam lidando com algo jamais visto no direito e não sabiam como se posicionar. A doutrina diverge a respeito do primeiro delito informático cometido, porém, majoritariamente, o primeiro crime teria ocorrido no ano de 1964, no Instituto de Tecnologia de Massachusetts (MIT - Massachusetts Institute of Technology) localizado na cidade de Cambridge, no estado de Massachusetts, nos Estados Unidos. A infração foi cometida por um aluno, de 18 anos de idade, que foi advertido pelos seus superiores.

Outros grandes casos escandalizaram a população, sendo o assunto mais falado das mídias durante muitas semanas, como o caso da empresa norte americana de seguros, a Equity Funding Corporation of America, localizada na cidade de Los Angeles, no estado da Califórnia, também nos Estados Unidos. O ano era 1973, e a empresa sofreu um prejuízo de mais de 30 milhões de dólares, indo à falência, em razão de uma fraude no seu sistema de processamento de dados que controlava as apólices de seguros. Outro caso emblemático seria o sucedido na Universidade de Oxford, localizada em Oxford, no Reino Unido, em 1978, onde um estudante realizou uma cópia de uma prova, através de uma rede de computadores. Seria uma invasão seguida de uma cópia.

Até aquele momento os estudiosos pensavam que as condutas criminosas cibernéticas atentavam apenas contra o âmbito econômico. A Alemanha, um dos países pioneiros na legislação contra essas práticas, apresentavam

movimentos iniciais no sentido de criminalizar as condutas que lesionavam a ordem econômica. Apenas a partir da década de 1980, após o Comitê Europeu concluir que tais condutas também violavam outros direitos, como o da privacidade, o da intimidade e os direitos autorais dos cidadãos, é que o mundo começou a se atentar para tanto.

Muitos estudiosos estiveram engajados no combate ao crime eletrônico no passado, como o americano Donn. B. Parker [4], um dos primeiros pesquisadores do cibercrime. Donn desenvolveu uma espécie de manual de aplicação de leis para as autoridades, denominado “Computer Crime - Criminal Justice Resource Manual”, criado em 1979 virando referência, até mesmo fora dos Estados Unidos. No âmbito europeu, o primeiro estudo acadêmico que se teve ciência, sobre crimes eletrônicos, foi apresentado por Ulrich Sieber, com sua obra intitulada “Computer criminalitatund strafrecht”. Já a primeira iniciativa internacional que tratava de cibercrimes foi a conferência sobre Aspectos criminológicos do crime Econômico, que aconteceu em Estrasburgo, na França, em 1978.

No entanto, foi nas décadas de 1980 e 1990 que os cibercrimes começaram a se popularizar. As condutas mais comuns na época eram a pornografia infantil, a disseminação de vírus, a invasão de sistemas e a pirataria. Tais condutas acabaram por iniciar um momento de conscientização voltada para a segurança dos sistemas, surgindo em um contexto em que já se falava sobre “guerra de informação”. É nesse período que o termo “Cybercrime” também se tornou conhecido, em meados da década de 1990, surgindo em Lyon, na França.

No Brasil, tem-se registrado com um dos primeiros crimes cibernéticos o crime de “phishing scam”, ou “pescaria de senhas”, no setor bancário, em 1999[5]. Outro caso igualmente célere que marcou o início dos crimes informáticos no País

[4] Disponível em: <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf>.
[5] Disponível em: <http://www1.folha.uol.com.br/fsp/cotidian/ff05089912.htm>.

ocorreu em 1997, quando a Justiça de Belo Horizonte tirava da internet fotografias de crianças em sexo explícito, sendo que o responsável por tal crime tinha apenas 15 anos à época do fato. A partir de então, muito se debateu sobre a problemática que envolvia a investigação de crimes informáticos, que poderia ser praticado por qualquer pessoa, em qualquer localidade, com uma facilidade maior. Começamos a refletir, também, sobre a necessidade de leis que tratassem de crimes cibernéticos, e quais bens jurídicos procuraríamos proteger.

Se faz mister, no presente histórico, colocar em voga o renomado HC 76.689/PB, relatado pelo Ministro Sepúlveda Pertence. Na época, o Supremo Tribunal Federal já enfrentava um caso que abrangia pornografia infantil nas antigas BBs (Bulleting Board System/Internet). Naquele estágio, já se poderia perceber a necessidade de lei específica para responder aos delitos. Mas, via contrária, o Ministro defendeu a tese de que nem todos os delitos cibernéticos necessitariam de uma nova tipificação, pois em muitos a tecnologia e a internet se configuravam apenas como o meio utilizado para a materialização de crimes já conhecidos e tipificados. Vejamos:

> "crime de computador': publicação de cena de sexo infantojuvenil (ECA, art. 241), mediante inserção em rede BBs/internet de computadores, atribuída a menores. tipicidade. Prova pericial necessária à demonstração da autoria: Hc deferido em parte.
>
> 1. o tipo cogitado – na modalidade de 'publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente' – ao contrário do que sucede por exemplo aos da Lei de imprensa, no tocante ao processo da publicação incriminada é uma norma aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBs/internet de computador.
>
> 2. não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta criminalizada, o meio técnico empregado para realizá-la pode até ser de invenção pos- terior à edição da lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo.
>
> 3. se a solução da controvérsia de fato sobre a autoria da inserção incriminada pende de informações técnicas de telemática que ainda pairam acima

> do conhecimento do homem comum, impõe-se a realização de prova pericial".[6]

Equivocado, por certo, estava o ministro. Como já afirmava em 1996 o autor Ivan Lira de Carvalho:

> "Sendo perguntado, por exemplo, se a internet é um meio novo de execuções de crimes 'velhos' ou é, por si mesma, uma geradora de novos delitos, terei o atrevimento de dizer que as duas partes da pergunta se completam para a resposta: há crimes novos, contemporâneos da formação da rede mundial de computadores, mas estão acontecendo, pela 'net', delitos já de muito tempo conhecidos da sociedade, só que agora perpetrados com o requinte do bit. Óbvio é que a lei deve acompanhar as inovações criadas e experimentadas pela sociedade. Mas, como na maioria dos sistemas jurídicos que têm a lei como fonte principal (é o caso brasileiro), o processo legislativo é bem mais lento do que os avanços tecnológicos e as consequências destes. No entanto, nem por isso os operadores jurídicos devem cruzar os braços, ficando no aguardo de providências legislativas compatíveis com a modernidade das técnicas criminosas. Se é possível o encaixe da conduta antissocial a um dispositivo legal em vigor, não deve o aplicador do Direito quedar-se em omissão" [7]

Já no ano 2000, em plena eleição, o ex-Prefeito Paulo Maluf se tornaria o primeiro político brasileiro vítima de sabotagem digital. No ano de 2002, o Brasil se tornaria conhecido pelo mundo como o maior "exportador" de criminalidade pela via da internet. Dois anos após, em 2004, viria a primeira condenação de pirataria virtual no Brasil, com a condenação de um jovem de 19 anos a seis anos e quatro meses de prisão, por aplicar golpes por meio da internet no Brasil e nos Estados Unidos [8].

O Brasil passou a se preocupar e a tratar o tema da criminologia informática nas últimas duas décadas. As primeiras leis que tratam do assunto são as Leis de nº12.735 e de nº12.737, ambas de 2012. Logo após, o Marco Civil da Internet é promulgado, na forma da Lei nº 12.965/2014, estabelecendo princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Quatro anos depois, no

---

[6] **JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 24

[7] **JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 25

[8] Confira alguns crimes virtuais que viraram notícia. Folha de S.Paulo, 7-1-2006. Disponível em: <www1.folha.uol.com.br/folha/informatica/ult124u19460.shtml>.

ano de 2018, nosso País incorpora ao Código de Processo Penal o Art. 216-B, que tipifica as condutas de “produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes”, o que traz uma maior segurança aos usuários da internet, no momento em que há um maior cuidado ao bem jurídico da intimidade do indivíduo frente à um ambiente em que tais condutas acabaram por se tornar banais. E, por fim, recentemente, foi promulgado a portaria de nº 69, de dois de maio de 2019, que institui um grupo de trabalho destinado a avaliar os parâmetros para o uso adequado das redes sociais pelos magistrados.

2.1) Estatísticas dos cibercrimes no Brasil e no mundo

Atualmente, o custo médio por vítima de crime cibernético, em dólares, é de U$ 128. São enviados, por dia no mundo, 75 milhões de e-mails suspeitos, sendo certo que cerca de 2.000 mil pessoas são vítimas diárias desses emails. Cerca de 73% de americanos já tiveram experiências com o cibercrime, e 78% acreditam que os cibercriminosos não serão punidos. Enquanto isso, apenas 2% de americanos acreditam que nunca serão vítimas de cibercriminosos[9].

Os dados relativos ao Brasil, como podemos perceber no início do presente capítulo, também se mostram bem alarmantes. Hoje, nosso País é o quarto no mundo com o maior número de ameaças virtuais[10].

E, infelizmente, não é novo o fato do Brasil apresentar altos índices de criminalidade tecnológica. Pesquisas sempre demonstraram que o Brasil é conhecido na rota dos crimes cibernéticos. De acordo com a Polícia Federal, em pesquisa realizada no ano de 2004, de cada 10 hackers ativos no mundo, 8 viveriam

---

[9]Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-05/cibercrimes-causaram-prejuizos-de-bilhoes-de-dolares-no-mundo-em-2016>

[10]Disponível em: <http://info.abril.com.br/noticias/seguranca/brasil-e-o-4-pais-com--maior-numero-de-ameacas-virtuais-04052012-16>.

no Brasil[11]. Ainda segundo a Polícia, à época, dois terços da totalidade dos criadores de páginas de pedofilia na internet, detectadas por investigações policiais brasileiras e estrangeiras, teriam origem brasileira[12]. E a mesma Polícia Federal já afirmou que o cibercrime já gera mais dinheiro do que o próprio narcotráfico[13].

Os crimes na internet atingiam, em 2011, 77 mil brasileiros por dia, gerando um prejuízo anual de 104 bilhões de reais, segundo levantamento feito pela Norton[14], empresa de segurança de computadores. Já o número de crimes virtuais no Brasil aumentou 70% entre os anos de 2012 e 2013, conforme dados do cnB (Colégio Notorial do Brasil)[15].

Líder global em segurança cibernética, a empresa Symantec afirma que entre os anos de 2011 e 2012 os cibercrimes teriam gerado um prejuízo de cerca de R$15,9 bilhões, valor esse que ultrapassa o identificado pela Federação Brasileira de Bancos (FE-BrABAn), que indicava um prejuízo de R$1,5 bilhão. Deste valor, cerca de R$900 milhões seriam decorrentes de apenas fraudes bancárias, como os golpes envolvendo cartões de crédito e débito[16].

No ano de 2005, em acórdão do STF, o Ministro Gilmar Mendes admite que os crimes cibernéticos existiam e eram realidade em nosso País. E diante dos altos índices demonstrados, a manifestação do Ministro era mais que necessária. Á título de ilustração, pode-se citar mais uma pesquisa, dessa vez realizada pelo

---

[11]Disponível em: <http://info.abril.com.br/aberto/infonews/092004/13092004-13.shl>.
[12]Disponível em: <http://agenciabrasil.ebc.com.br/noticia/2004-09-13/pesquisas-apontam-que-brasil-esta-na-rota-dos-crimes-na-internet>.
[13]Disponível em: <http://g1.globo.com/noticias/rio/0,,MUL487856-5606,00-CRIMEs+VIRTUAIS+GERAM+MAIS+DINHEIRO+DO+QUE+O+NARCOTRAFICO+DIZ+PF.html>.
[14]Disponível em: <http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/09/20/crimes-ciberneticos-atingem-77-mil-brasileiros-diariamente-prejuizo-e-de-r-104-bilhoes. jhtm>
[15]Disponível em: <https://www.techtudo.com.br/noticias/noticia/2014/10/registros-de-ocorrencias-de-crimes-virtuais-aumentam-70-no-pais-em-1-ano.html>.
[16]Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/10/crime-cibernetico-gera-prejuizos-de-quase-r-16-bilhoes-no-brasil.html>

Instituto de segurança cibernético Ponemon[17]. A pesquisa, intitulada como “Cost of a Data Breach 2018”, revela que as empresas brasileiras são, dentre outras, as empresas que têm maiores chances de sofrer ataques cibernéticos. O estudo demonstra que a probabilidade de uma dessas empresas brasileiras sofrer algum tipo de violação de seus registros virtuais chega a 43%, o que representa uma piora significativa, se relacionado à médias dos últimos 5 anos, que era de 38%. No mundo, a probabilidade de violações de dados cibernéticos chega a média de 27%.

A mesma pesquisa também levou em conta o tempo médio para identificar uma violação de dados. O tempo médio, mundial, é de 197 dias, sendo que o tempo para conter a violação seria de 69 dias. Já no Brasil, são necessários 240 dias para identificar a infração e cerca de 100 dias para conter a violação de dados. E quando o cibercrime é causado por hackers, o que representam cerca de 46% dos casos ocorridos aqui no Brasil, o custo e o tempo para dar fim à ameaça são ainda maiores[18].

O Brasil é destaque também nos crimes conhecidos como “Phishing”, ou pescaria de senhas. Nosso País, atualmente, é o quarto principal alvo dos crackers em ataques dessa natureza, figurando entre os cinco países que mais tiveram empresa hackeadas. O Brasil chega a marca de cerca de 38 milhões de usuários lesados[19].

A média mensal dos crimes informáticos em que as vítimas eram crianças cresceu 57% em 2012[20]. No ano seguinte, o Brasil perdeu U$$ 8 bilhões com roubos

---

[17]Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/07/custo-com-violacao-de-dados-no-brasil-e-o-menor-do-mundo.html>.
[18]Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/07/custo-com-violacao-de-dados-no-brasil-e-o-menor-do-mundo.html>.
[19]Disponível em: <http://seumicroseguro.com/2013/06/23/brasil-e-o-4o-principal-alvo--dos-crackers-em-ataques-phishing-no-mundo/>.
[20]Disponível em: <http://olhardigital.uol.com.br/negocios/digital_news/noticias/ataques--de-phishing-atingem-38-milhoes-de-usuarios,-diz-kaspersky>.

de senhas, pirataria virtual, ataques de crackers e clonagens de cartões, abrangendo até mesmo condutas como espionagem governamental e industrial, dentre outras condutas que entrariam no âmbito das infrações tecnológicas[21]. Cerca de 57% dos usuários de smartphones no País foram vítimas de crime virtual móvel (GONZAGA, 2013).

Os números e estatísticas foram apresentados à título de ilustração. Meramente exemplificativos, demonstram para nós o quão preocupante é tal realidade, evidenciando a necessidade de tipos penais que efetivamente protegem os bens jurídicos dos usuários. Partimos de lesões individuais, como o vazamento de uma foto íntima na internet, até situações em que grandes empresas se comprometem e perdem bilhões prejudicando a economia brasileira. O bem jurídico da privacidade precisa ser protegido frente aos riscos da sociedade da informação.

[21]Disponível em: <http://brasileconomico.ig.com.br/tecnologia/2014-06-09/crimes-de--informatica-custam-cerca-us-500-bi-para-economia-mundial.html>.

3) DIREITO COMPARADO

É inegável, nos presentes dias, o fato de que somos completamente dependentes das novas tecnologias da informação, principalmente no que diz respeito à informática e a internet. O ciberespaço é utilizado nos mais variados âmbitos na vida do indivíduo usuário: cada vez mais comum atualmente, as relações interpessoais têm começado (e se mantido) através da internet, o comércio é virtual, contas podem ser pagas através de aplicativos desenvolvidos para smartphones e até mesmo o governo já pode ser eletrônico, como o “e-government”. Todas essas mudanças (e suas consequências) implicam em uma espécie de criminalidade moderna, que deve ser analisada à luz do contexto social atual, que se desenvolveu e se resultou na chamada “Sociedade de Informação”.

Pelo fato do ciberespaço abarcar tantas áreas da vida de um sujeito e por ser um ramo consideravelmente novo no âmbito jurídico, houve e ainda há dificuldade na regulamentação dos crimes cibernéticos. Tais crimes se desenvolvem muito rápido, se adaptando e acompanhando a evolução da tecnologia. Além disso, os mesmos atingem a coletividade e podem ser propagados por vários Países, o que gera um grande conflito jurisdicional.

A matéria de combate aos cibercrimes atinge todo o cenário mundial. Vivemos uma situação em que nenhum País é autossuficiente no combate aos crimes tecnológicos, uma vez que não adiantaria regulamentar a matéria apenas na esfera interna de cada Estado, pois, como já exposto anteriormente, se trata de matéria complexa que possui implicações em escalas globais.

De forma a conjugar esforços no combate aos cibercrimes, foram realizadas algumas convenções internacionais, como por exemplo a Convenção de Bruxelas e a Convenção de Haia de Direito Internacional Privado. A mais relevante e

significativa é a Convenção de Budapeste (Convenção sobre Cibercrime do Conselho da Europa), que será tratada mais detalhadamente a seguir.

3.1) Convenção de Budapeste

A Convenção de Budapeste foi celebrada em 23 de novembro de 2001 e se trata de documentação de Direito Internacional Público, realizada por um comitê de especialistas e teve como objetivo a implantação, nos países signatários, de normas de direito material que efetivamente combatem os crimes cibernéticos.

A Convenção teve como total de signatários 43 países, sendo em sua maioria Europeus, contando também com a adesão de países como os Estados Unidos, Canadá, África do Sul e Japão. O respectivo acordo internacional fixou diretrizes às políticas nacionais das nações participantes, no sentido de harmonizar suas legislações para um combate mais eficiente e efetivo contra os crimes praticados no ciberespaço. A Convenção também consolidou todas as recomendações e orientações anteriores no tocante à tipificação dos delitos informáticos, feitas pela Comunidade Européia e pela Organização das Nações Unidas (ONU)[22].

A Convenção de Budapeste foi dividida em quatro partes, sendo: terminologia; providências adotadas em circunstâncias nacionais; cooperação internacional e disposições finais. Apresentou também 5 títulos. Em seu título I, a Convenção estabelece as infrações que deverão ser tipificadas no no âmbito do direito interno de cada signatário, que atentam contra, por exemplo, a

[22]Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf>.

confidencialidade, a disponibilidade de sistemas e dados informáticos, e à integridade[23].

As condutas que se sucedem na internet, como a falsidade informática (introdução, alteração, eliminação, ou supressão de dados informáticos produzindo dados não autênticos, com a intenção de que estes sejam utilizados para fins legais como se autênticos fossem), e a burla informática (que pode ser entendida como qualquer espécie de intervenção no sistema informático) são tema do Título II da Convenção[24].

Infrações referentes ao conteúdo, como as condutas que estão relacionadas à pornografia infantil, se caracterizam como matéria do Título III. Já o Título IV trata das infrações relacionadas com a violação do direito do autor e dos direitos conexos[25].

Afinal, o Título V elenca as hipóteses de responsabilidade e as sanções respectivas as mesmas, como os artigos referentes à ”Tentativa e Cumplicidade”, e “Responsabilidade de pessoas colectivas” [26].

Se faz importante salientar que a presente Convenção ainda destaca a necessidade de cooperação entre os países signatários, ao instituir princípios e diretrizes que devem ser seguidos pelos Estados membros, objetivando que nenhum comportamento previsto fique impune, sugerindo também certos tipos de

---

[23]**BARROS, Marco Antônio de; CONTE, Christiany Pegorari e GARBOSSA, Daniella D’Arco.** Crimes informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar. Pg. 415.
[24]**BARROS, Marco Antônio de; CONTE, Christiany Pegorari e GARBOSSA, Daniella D’Arco.** Crimes informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar. Pg. 415.
[25]**BARROS, Marco Antônio de; CONTE, Christiany Pegorari e GARBOSSA, Daniella D’Arco.** Crimes informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar. Pg. 415.
[26]**BARROS, Marco Antônio de; CONTE, Christiany Pegorari e GARBOSSA, Daniella D’Arco.** Crimes informáticos e a Proposição Legislativa: considerações para uma reflexão preliminar. Pg. 415.

procedimentos em casos de vacância de acordos internacionais que tratem do assunto.

Por fim, a Convenção discorre ainda de questões relativas à extradição, da assistência mútua entre os Estados, da definição de confidencialidade, das chamadas denúncias espontâneas e também da definição de conceitos como “confidencialidade” e “limitações de uso”. Além disso, a Convenção admite também a admissão de Estados que querem ser signatários, através de convites feitos pela própria convenção e aprovação por maioria do Conselho.

O Brasil, por sua vez, não aderiu à Convenção de Budapeste. Com as Leis nº12.735/2012 e nº12.737/2012 e, mais recentemente, com a promulgação do Art. 216-B do Código Penal, nosso país avança rumo à uma proteção mais efetiva da privacidade e da intimidade dos usuários da rede mundial de computadores, se aproximando à conformidade imposta pela dita Convenção. Mesmo o Brasil não sendo um dos países signatários da Convenção, é inquestionável que as resoluções e diretrizes definidas na mesma estimularam os debates sobre o assunto em nosso País, como podemos verificar analisando o Projeto de Lei nº2.793/2011, que resultou na Lei nº12.737/2012. Averigua-se que há forte influência sobretudo do Título I do documento, que versa sobre temas como integridade, confidencialidade, disponibilidade dos sistemas informáticos e dos dados cibernéticos.

3.2) Direito Penal Informático no Mundo

Sem a pretensão de esgotar o assunto, a presente obra apresenta, a seguir, uma breve síntese de alguns países do mundo que vêm legislando sobre a criminalidade informática.

3.2.1) Estados Unidos

Os Estados Unidos se apresentam como um dos primeiros países a legislarem sobre os cibercrimes. Tal país ficou conhecido por ser um dos pioneiros na luta à criminalidade na internet. Os debates acerca do tema já se iniciavam na década de 1970, tendo nos dias atuais leis específicas que discorrem sobre o assunto[27].

As leis americanas punem casos de acesso indevido, sabotagem informática e até interceptação não autorizada em computadores. Vários capítulos do “United States Code”, o “Código Penal Americano” tipificam condutas do âmbito informático, como o capítulo 47, presente na Parte I do título 18, que trata de fraude e declarações falsas. A seção 1.030, inclusive, compreende os crimes que envolvem fraudes e condutas relacionadas à conexão na web (conceitua a Lei Federal Americana “Fraude de Computador” como o uso da internet com o intuito de criar uma deturpação desonesta de um fato como meio à compelir alguém a fazer ou deixar de fazer algo que lhe provoque uma perda)[28] .

No ano de 1994, o Código Penal Federal Americano foi modificado pela Lei de Crimes Violentos, a “Violent Crimes Act”. Tal alteração tipificou condutas como a disseminação de vírus, danos aos sistemas e seus dados e a interceptação telemática. Sete anos depois, em 2001, a lei estadunidense foi mudada novamente, sendo emendada dessa vez pela Lei Patriótica, a “USA Patriot Act”, que, com o objetivo de combater práticas terroristas, supre o Governo com um embasamento legal que possa efetivamente monitorar o que é feito na rede[29].

---

[27] **JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 62

[28] Um compilado sobre disposições acerca do cibercrime nos Estados Unidos pode ser aces- sado em: <http://www.oas.org/juridico/spanish/us_cyb_laws.pdf>.

[29] **JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 63

A Lei Federal, porém, possui papel secundário no cenário jurídico americano. Cada Estado do respectivo País pode criar a sua própria legislação em matéria penal.

Por fim, cabe salientar que os Estados Unidos apresentou recentemente dois projetos de leis federais que criminalizam a disseminação não consentida de imagens íntimas. Trinta e oito dos cinquenta estados americanos já tipificam a conduta. Além disso, o País também possui um artigo no "Communications Decency Act", que se caracteriza por ser a primeira tentativa notável do Congresso Americano no sentido de regulamentar a pornografia dissipada na internet. O respectivo artigo limita a responsabilidade de possíveis intermediários quando ao material de terceiros no que diz respeito à exposição de mulheres adultas. A Lei Geral que cuida do assunto é chamada de "Communications Decency Act", e os dois projetos de "Protecting the Rights of Individuals Against Technological Exploitation Act-(HR 2052)" e "Intimate Privacy Protection Act"[30].

3.2.2) Alemanha

A Alemanha é identificada como um dos primeiros países a refletir sobre as alterações necessárias relativas aos crimes praticados na web. Desde meados da década de 1980, a legislação germânica abrange alguns tipos de comportamentos cibernéticos, como a fraude informática, a espionagem, a falsificação e alteração de dados e a sabotagem informática, em sua Lei de Criminalidade Econômica. Já em 2006, o Governo alemão propôs um novo projeto que buscava renovar as leis informáticas que já existiam[31].

---

[30]Disponível em: http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[31]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 64

No Código Penal alemão hodierno, o chamado “Strafgesetzbuch”[32], se encontram a seção 202a, que aborda condutas de espionagem, a seção 303a, que trata de crimes que envolvem alterações de dados, e a seção 303b, que expõe sobre os crimes de sabotagem informática[33].

Recentemente, em 2014, a Alemanha apresentou um novo projeto de Lei, que trata sobre segurança cibernética, objetivando a proteção da infraestrutura do país e a proteção da sociedade como um todo.

Já em relação à proteção da intimidade e da privacidade do usuário no ciberespaço, a Corte Federal de Justiça Alemã tomou uma importante decisão. A Alemanha tipifica condutas que violem a privacidade íntima do indivíduo, na forma de fotos e/ou vídeos. As condutas tipificadas incluem a proibição da divulgação ilegal das mídias a terceiros, mesmo que, no momento em que a foto foi tirada ou o vídeo gravado, houvesse o consentimento. O País decidiu em caso específico que imagens de ex-parceiros(as) devem ser deletadas se requisitado, pois, do contrário, acarretaria em uma intensa violação de privacidade. A lei, no caso é a “VI ZR 271/14 (BGH, Urteil vom 13. Oktober 2015 – VI ZR 271/14 – OLG Koblenz)”[34].

3.2.3) Filipinas

No ano de 2009, entrou em vigor no País a lei denominada de “Anti-Photo and Video Voyeurism Act of 2009”[35], que criminaliza o ato de tirar uma foto ou de gravar alguém que se encontra em situação sexual ou similar. O mesmo cabe às imagens e vídeos que demonstram as partes íntimas dos indivíduos. É uma das primeiras leis específicas que versam sobre a intimidade do internauta.

---

[32]Disponível em: <http://www.gesetze-im-internet.de/stgb/index.html>.

[33]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 64

[34]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[35]Acesso à legislação em: <http://www.senate.gov.ph/lisdata/111349486!.pdf>.

Já em 2012, o senado das Filipinas aprovou a redação final da referida lei, inserindo novos tipos de condutas, como o “cybersex” (entendido como “sexo virtual”) e o “cybersquatting” (que seria considerado como o registro, tráfico, ou utilização de um nome de domínio com com o intuito de obter vantagens econômicas provenientes do uso de uma marca pertencente a terceiros)[36].

3.2.4) Itália

Foi entre os anos de 1992 e 1993 que as discussões sobre os cibercrimes começaram no país, com a edição do Decreto Legislativo nº 518, de 29 de dezembro de 1992, e com a Lei nº 547, de 23 de dezembro de 1993. Esses primeiros marcos legislativos ampliaram a redação de tipos penais já existentes para abranger os novos crimes informáticos. Condutas como fraudes informáticas (que se constituem na alteração de dados em sistemas de terceiros ao buscar a obtenção de vantagem ilícita) e a sabotagem informática (prática que compromete a funcionalidade do sistema informático) passaram a ser criminalizadas[37].

À título de ilustração, pode-se citar o art. 615 do Código Penal italiano, dos crimes contra a inviolabilidade de domicílio. O tipo em questão foi ampliado para incorporar casos que envolvem as “invasões de iP”, visando sempre o dano em sistema de outrem. Na concepção legislativa italiana, portanto, a invasão de computadores e o acesso à seus dados privados seria considerado uma espécie de violação de domicílio.

---

[36]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[37]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 64

3.2.5) Índia

Uma importante fonte legislativa indiana que versa sobre os cibercrimes é o “The Information Technology Act (21/2000)”, que pune os “hackers” com uma pena superior a três anos. As condutas de sabotagem e alteração indevida de sistemas informáticos também são tipificadas pela lei [38].

A Índia não possui lei ou projeto de lei específico no sentido de proteger a privacidade do indivíduo frente a divulgação de imagens íntimas na web. Lado outro, algumas de suas leis podem ser aplicadas por analogia em alguns casos que tratem do assunto. A legislação indiana é bastante rígida quanto à disseminação de imagens de menores de idade na rede.

Suas leis gerais são a “Information Technology Act 2000”, a “ Indian Penal Code” e “The Protection of Children from Sexual Offenses Act”[39].

3.2.6) Japão

O Japão regulamentou a matéria dos cibercrimes através da lei nº128/99, chamada de “Unauthorized Computer Access Law”. A matéria também é tratada pelo Código Penal japonês, em seus artigos 258 e 259. Algumas das condutas tipificadas incluem a relevação de senhas e invasões de dispositivos informáticos, e as penas correspondentes variam entre trabalhos forçados e multas pecuniárias[40].

O País, visando à proteção da privacidade do usuário, promulgou a lei chamada de “Revenge Porn Victimization Prevention Act”, que torna crime o ato de

---

[38]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 65

[39]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[40]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 65

publicar imagens sexuais que possam incomodar e constranger a vida privada de terceiros. É necessário que a vítima não tenha consentido nem autorizado o uso de sua imagem[41].

3.2.7) França

É presente, no País, desde 1988, disposições sobre os crimes na internet. É do mesmo ano a Lei nº19, que criminalizam ações como a sabotagem informática, a falsificação de documentos em cyber plataformas, o acesso fraudulento a um banco de dados, a falsificação de seu sistema de tratamento e, por fim, a destruição e a adulteração de dados. Posteriormente, em 2004, foi promulgada a Lei nº 575 , de 21 de junho do mesmo ano[42], que confere proteção ao comércio na internet, tratando também de punições a fraudes correspondentes.

A França aderiu à convenção Européia de Cibercrimes em 10 de janeiro de 2006. Desde então, o País passou a criminalizar os atos de desenvolver e fornecer ferramentas, equipamentos, códigos e softwares utilizados para a prática dos crimes virtuais[43].

Recentemente, em outubro de 2016, a França, com o intuito de proteger a intimidade dos internautas, promulgou a lei denominada de “Loi pour une République Numérique”, que modifica o Código Penal francês no sentido de criminalizar a divulgação e a publicização de documento escrito ou imagens de cunho sexual. A

---

[41]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[42]Íntegra da legislação em: <http://www.legifrance.gouv.fr/affichtexte.do;jsessionid=4E472cDE49F1945cFD9516c29A2B1B21.tpdila09v_1?cidtexte=JorFtEXt000000801164&datetexte=20150623>.

[43]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 65

conduta é criminalizada na legislação francesa independentemente do consentimento e da autorização da vítima, sendo expressa ou presumida[44].

3.2.8) Inglaterra

Um dos países pioneiros no combate aos cibercrimes, desde o ano de 1984 a Inglaterra já possuía a chamada "Data Protection Act", que ficou conhecida como a lei que conferia proteção aos dados pessoais do usuário no âmbito cibernético. Já na década de 1990, foi introduzido ao ordenamento jurídico inglês o crime de acesso não autorizado com o intuito de adulterar o conteúdo presente na plataforma. A legislação inglesa influenciou a brasileira (como se pode verificar na Lei nº12.737/2012) no sentido de punir condutas que tenham como finalidade a alteração das informações presentes no sistema, independentemente do resultado[45].

Se contrapondo a legislação brasileira, a lei inglesa fixa parâmetros e apresenta condutas que, se praticadas, indicam o elemento doloso e a provável intenção de adulterar conteúdo presente na web. Tais diretrizes retratadas não existem no quadro de leis brasileiras, ficando a cargo da interpretação dos magistrados.

Foi em 29 de agosto de 1990[46] que se promulgou uma das mais relevantes leis em termos de direito penal informático, a chamada "Computer Misuse Act". A mesma foi alterada 16 anos após, pelo "The Police and Justice Act 2006".

Já em relação à legislação inglesa no País de Gales, se faz mister informar que a mesma trata de vários crimes, como o acesso indevido aos sistemas informacionais e a produção de sistemas e de códigos de acesso que possam

---

[44]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[45]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 66

[46]Legislação acessível em: <http://www.legislation.gov.uk/ukpga/1990/18/contents>.

facilitar e permitir a invasão. Há pouco tempo, no ano de 2014, foi proposto no Parlamento inglês onze novas leis, se destacando a “Serious Crime Bill”, que altera em substância a lei de 1990 no sentido de prever penas de prisão perpétua para os agentes de crimes cibernéticos.

No ano posterior, em 2015, entra em vigor o “Criminal Justice and Courts Act 2015”, o qual incorpora ao quadro legislativo do Reino Unido (Inglaterra, País de Gales e Irlanda do Norte) novas condutas que ferem a privacidade do indivíduo usuário, como a ato de revelar fotos e filmes sexuais privados, tendo a intenção de constranger e angustiar a vítima[47].

3.2.9) Portugal

A legislação portuguesa criminaliza o acesso indevido aos sistemas informáticos desde o ano de 1991, com a promulgação da Lei nº 109. Dentre os delitos previstos, estão as condutas de dano informático, falsidade cibernética, interceptação informática, sabotagem no âmbito da internet, reprodução fraudulenta de programas de computador, dentre outros. É classificado como qualificadora a conduta executada com a quebra de segurança[48].

Recentemente, entre os anos de 2015 e 2016, o País teve importantes decisões judiciais que definiram se haveria possibilidade de indenização para as vítimas que tiveram conteúdo íntimo divulgado por falha de segurança do sistema.

O País avança em condutas de proteção ao utilizador da rede quando apresentou projetos de lei que incluíam agravantes na conduta de disseminar

---

[47]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[48]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 67

imagens íntimas nos crimes de violência doméstica, nos crimes contra intimidade da vida privada e no crime de gravações e fotos ilícitas e/ou íntimas[49].

3.2.10) Espanha

Em meados da década de 1990, o código Penal espanhol foi modificado, ao prever várias disposições relativas aos cibercrimes. Dentre alguns delitos, destacam-se os crimes de violação de privacidade com o intuito de obter informações íntimas do internauta, que apresentam como pena a prisão de um a quatro anos e multa que varia entre doze e vinte e quatro meses [13], o crime de alteração indevida de dados e a fraude informática, que é tido como o crime de estelionato no Brasil, dentre outros[50].

No ano de 2015, o Código Penal espanhol passa a criminalizar a divulgação de fotografias tiradas em ambiente privado a terceiros, sem a autorização e consentimento. A legislação espanhola ainda possui a chamada “Lei Orgânica de Proteção de Dados de Caráter pessoal”, que possibilita o pedido de retirada de conteúdo íntimo da web se o mesmo se apresentar inadequado, excessivo e ofensivo à privacidade do internauta[51].

A Agência Espanhola de Proteção de Dados possui a prerrogativa de retirada de conteúdo indevido de sites europeus, impedindo inclusive o acesso a conteúdos na rede dentro da Espanha.

---

[49]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

[50]**JESUS, Damásio de.** Manual de crimes informáticos / Damásio de Jesus,José Antonio Milagre. – São Paulo : Saraiva, 2016. Pg. 67

[51]Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>.

4) Das fontes legislativas penais brasileiras

A presente obra irá dissertar, a seguir, sobre as principais fontes legislativas penais brasileiras que tratam dos cibercrimes.

4.1) Lei nº 12.735 de 2012

A Lei de nº12.735, de 30 de novembro de 2012, procedeu do Projeto de Lei nº 84/99 (89/2003) e foi planejada, inicialmente, para ser extravagante. A mesma, porém, foi modificada e promoveu alterações no Decreto-Lei nº 2.848, de 07/12/1940, o Código Penal Brasileiro, no Código Penal Militar (Lei nº7.716, de 05/01/1989) e na Lei nº 7.716, de 5 de janeiro de 1989. Segue a mesma:

> "LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.
>
> Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
>
> A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
> Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal , o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar , e a Lei nº 7.716, de 5 de janeiro de 1989 , para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
> Art. 2º (VETADO)
> Art. 3º (VETADO)
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989 , passa a vigorar com a seguinte redação:
> "Art. 20. .....
> .....
> § 3º .....
> .....

> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> ....." (NR)
> Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
>
> Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.
> DILMA ROUSSEFF
> *José Eduardo Cardozo*
> *Paulo Bernardo Silva*
> *Maria do Rosário Nunes*
> Este texto não substitui o publicado no DOU de 3.12.2012." [52]

A respectiva lei, apesar de tratar em seu preâmbulo condutas típicas que são realizadas mediante uso de sistema eletrônico, digital ou similares, e que foram praticadas também contra sistemas informatizados e similares, não acrescentou nenhum novo tipo penal ao ordenamento jurídico brasileiro, servindo apenas para alterar a legislação penal vigente.

A criação da Lei nº 12.735/2012 teve como influência preponderante a impossibilidade de proteção efetiva aos bens da vida, frequentemente lesionados pelos cibercrimes. O âmbito cibernético facilita a prática de delitos já conhecidos, além de propiciar condutas que antes eram improváveis de acontecer, como por exemplo a invasão de dispositivo informático.

Dessa maneira, os crimes cometidos na rede maculam de forma constante bens jurídicos fundamentais do ser humano, como a privacidade e a intimidade, se adaptando e se desenvolvendo rapidamente, ao acompanhar a evolução da tecnologia e da sociedade da informação. Assim, a respectiva lei preferiu buscar a proteção do indivíduo usuário através de uma legislação da década de 1940, ano da criação do Código Penal, em vez de tentar solidificar, no ato legislativo, condutas e comportamentos cibernéticos que são modificados de forma frequente, correndo o risco de se tornar defasada em um curto período de tempo.

[52]Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>

Apesar da Lei nº 12.735/2012 não ter adotado uma conduta própria e típica, existem leis específicas que tratam do assunto. As mesmas, entretanto, acabam por não conseguir abranger todo o âmbito em que os cibercriminosos atuam. Chega-se à conclusão de que ainda não é suficiente o arcabouço dos cibercrimes tipificados no ordenamento jurídico brasileiro. Nessa linha, se faz importante o entendimento de Alexandre Atheniense:

> "entendo que as soluções legais a serem buscadas deverão objetivar a circulação de dados pela internet, controlando a privacidade do indivíduo sem cercear o acesso a informação. Neste sentido é necessário aprimorar nossas leis de proteção de dados, inclusive com a regulamentação da atividade dos provedores que controlam a identificação do infrator, bem como um maior aparelhamento das delegacias especializadas"[53].

A lei analisada teve o intuito de preencher lacunas legislativas presentes em atos normativos já existentes, que impediam a tipificação dos crimes que são praticados pelos meios cibernéticos. Nesta oportunidade, a lei nº 12.735/2012 busca efetivar os princípios norteadores do Direito Penal, como o da legalidade e o da proibição de analogia.

A fonte legislativa em voga acerta na intenção, tendo como foco a proteção de direitos fundamentais como a privacidade, a intimidade e a informação, mas falha por ainda ser bastante genérica, não tipificando os novos delitos que o âmbito cibernético agora nos proporciona, em grande monta. Devem ser criados mecanismos específicos no combate aos crimes na web, para que se possa proteger tais bens jurídicos de forma efetiva. O mundo da internet e seus riscos ainda apresenta um certo vazio normativo frente ao ordenamento jurídico brasileiro.

Entende-se, portanto, que apenas a criação da Lei nº 12.735/2012 não é suficiente para coibir as práticas do criminoso no âmbito da web. Há a necessidade de uma regulamentação mais específica, o que está sendo recentemente abordado pela sociedade. Se faz importante, deste modo, citar o chamado “Marco Civil da

---

[53] **ATHENIENSE**, 2004, pg. 1.

Internet", a Lei de nº 12.965/2014, que se consiste em um tipo de "Constituição" da internet, que contém princípios e diretrizes que norteiam o uso correto da internet no Brasil, além de fornecer orientações também para o Poder Público no sentido de buscar o desenvolvimento positivo e benéfico da internet no Brasil. (WANDERLEI, 2012, p. 38-39).

4.2) Lei nº 12.737 de 2012

Nosso País não possuía legislação específica que tratasse dos cibercrimes até a aprovação da Lei nº 12.737/2012, conhecida como "Lei Carolina Dieckmann", procedente do Projeto de Lei nº 2.793/2011.

Após o famoso ocorrido com a atriz Carolina Dieckmann, caso que teve forte repercussão midiática, onde a atriz teve suas fotos íntimas divulgadas no ciberespaço sem sua autorização, as discussões que haviam no Brasil acerca da utilidade e da conveniência da criação de tipos penais cibernéticos chegou ao fim. Vêm, a esse cenário, a promulgação da Lei nº 12.737/2012 que, ao contrário da Lei de nº 12.735/2012, elenca novos tipos penais, trazendo também importantes alterações legislativas.

A criação da respectiva lei se caracteriza com um importante avanço à proteção da privacidade do internauta, visto que os primeiros estudiosos do tema muitas vezes confundiam o objeto do crime com o meio de prática do mesmo. Nesse sentido, se faz importante a lição de MIRANDA[54]:

> "Poderíamos citar, a título ilustrativo, alguns crimes atualmente perpetrados com o uso de alta tecnologia: O estelionato em todas as suas formas, lavagem de dinheiro, os crimes do colarinho branco, furto, a modalidade conhecida por "salami slicing" (fatiamento de salame, em que o ladrão faz regularmente transferências eletrônicas de pequenas quantias de milhares de contas para a sua própria, muitas vezes camuflada por campanhas de

[54]**MIRANDA, Marcelo Baeta Neves.** Abordagem dinâmica aos crimes via internet. 1999. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=1828>.

> arrecadação de donativos de modo a não despertar suspeitas), serviços subtraídos, o contrabando, a pornografia infantil, parafilia, invasões de privacidade, apologia de crimes, violações à propriedade intelectual ou industrial, violações à Lei do Software, pixações em sites oficiais do governo, vandalismo, sabotagem, dano, propagação de vírus de computador, a pirataria em geral, espionagem, tráfico de armas e drogas, lesões a direitos humanos (terrorismo, crimes de ódio, racismo, etc), destruição de informações, jogos ilegais, dentre inúmeros outros, apenas para explicitar a complexidade da matéria tratada.A experiência tem mostrado quão delicada é uma investigação de crimes por computador, seja pela falta de experiência policial, seja pela adoção de procedimentos desatualizados para a alta tecnologia empregada."

A fonte legislativa em análise, portanto, representa uma inovação para o nosso ordenamento jurídico, mesmo se encontrando distante da atuação ideal. É certo que a ausência de leis específicas, juntamente com práticas defasadas, estimulava o cibercriminoso a realizar os mais variados delitos na rede, sempre resguardado pelo anonimato presumido. Tínhamos, assim, milhões de brasileiros lidando diariamente com uma tecnologia que se desenvolve de maneira célere, sem conhecer os riscos provenientes e o principal, a existência de crimes nesse âmbito.

À título exemplificativo, foi realizada em 2012 pesquisa que comprova que cerca de 30% dos usuários mundias da web não se importavam com os crimes virtuais, nem mesmo sabendo o que os estes significariam.[55] Nesse paradigma, o ambiente informático brasileiro não se diferenciava daqueles vistos ao redor do mundo, sendo inclusive âmbito propício para a atuação dos criminosos digitais.

Frente à tal cenário, o ordenamento jurídico brasileiro se viu "forçado" a enquadrar as lesivas condutas cibernéticas em tipos penais já existentes, como aquele que pode criminalizar o indivíduo que adultera ou destrói dados da internet, se enquadrando ao Art. 163 do Código Penal, ou aquele que copia ou move, de forma indevida, informações presentes na Web, adaptando-se ao caput do Art. 155 do Código Penal Brasileiro. Claro que, diante de tais adequações equivocadas, os juristas brasileiros passaram a debater a questão à luz da "analogia in malan

[55]Disponível em: <http://www.teletime.com.br/04/10/2012/perdas-com-cibercrimes--chegam-a-r-15-bilhoes-no-brasil-por-ano/tt/304178/news.aspx>.

partem” que se aplicaria, segundo o professor Danilo Fernandes Christófaro [56],em caso de omissão do legislador quanto à determinada conduta, sendo a analogia in malam partem aquela que adota lei prejudicial ao réu, reguladora de caso semelhante. O princípio da reserva legal também influiu nos debates, sendo aquele que afirma que “nenhum fato pode ser considerado crime se não existir uma lei que o enquadre no adjetivo criminal. E nenhuma pena pode ser aplicada se não houver sanção pré-existente e correspondente ao fato.”[57]

O tipo que mais nos merece atenção, por ser o mais questionável e problemático da lei em questão, que será analisado a seguir, é o tipo intitulado como “Invasão de dispositivo informático”, presente no Art. 154-A. Percebe-se que tal artigo acabou por tipificar crimes característicos da esfera informática, como a invasão de dispositivo, a obtenção, destruição e adulteração de dados e a instalação e/ou disseminação de códigos cibernéticos dissimulados. Há a tipificação das formas qualificadas do crime, assim como suas majorantes. Mas a Lei acaba por se esquecer de adequar alguns tipos penais já existentes aos meios informáticos.

Se faz necessária a posição de entendimento positivo à criminalização de condutas típicas ao domínio virtual, em respeito ao Princípio da Legalidade e o da Segurança Jurídica. As condutas criadas pelo Art. 154-A buscam proteger a privacidade dos titulares dos dispositivos informáticos contra novas práticas ilícitas, que nem sempre podem ser ressarcidas civilmente.

Portanto, tem-se a penalização de novas condutas que lesionam a privacidade do internauta, tendo como objeto material a informática. O legislador acabou por tentar resumir a matéria principal analisada pela “Convenção de Budapeste” em apenas um tipo penal. Ocorre, todavia, que o legislador o fez de

[56]Disponível em: <https://lfg.jusbrasil.com.br/noticias/1064639/o-que-se-entende-por-analogia-in-malam-partem-danilo-fernandes-christofaro>.
[57]Disponível em: <https://www.jusbrasil.com.br/topicos/293139/principio-da-reserva-legal>.

forma atécnica, ao tipificar práticas já criminalizadas por outros artigos de nosso Código Penal, fazendo ainda o uso de expressões ambíguas em sua composição.

Por fim, percebe-se que a Lei nº 12.737/2012 ainda está longe de pacificar a questão dos cibercrimes, isto porque, como veremos, a punição pré-estabelecida diz respeito apenas à invasão dolosa, pouco importando quais consequências essa prática ilícita pode causar.

4.2.1) Análise do Tipo Penal

"Invasão de dispositivo informático"

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

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

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

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

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

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

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

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

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

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

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

Primeiramente, se faz importante o entendimento de qual (ou quais) bem(s) jurídico(s) penal(is) seria(m) resguardado(s) pelo Art. 154-A de nosso Código Penal. Tal matéria foi alvo de muitas discussões pelos juristas brasileiros. A princípio, os mesmos acreditavam que o respectivo delito, que ainda não tinha sido normatizado, gozava de conteúdo puramente patrimonial e econômico, se atendo à prática de furto de dados. Mas, segundo GOMES[58], os mesmos estavam equivocados, pois

> "o furto é um crime material onde há a diminuição do patrimônio do sujeito passivo, e, em contrapartida, um aumento do patrimônio do sujeito ativo. Quando um arquivo é furtado de outro computador, não é uma diminuição patrimonial pois o mesmo não é retirado da posse do sujeito passivo. na verdade, o arquivo é copiado por aquele que comete o ato [...] não há subtração e, por conseguinte, não há o furto."

Com a intensa evolução tecnológica e a popularização do acesso à internet, o crescimento dos cibercrimes se dava de forma muito célere. Tal fato acabou por provocar a atenção de mais especialistas no assunto, que acabaram por

[58]**GOMES, Ricardo Reis.** Crimes Puros de Informática.

conceber a tese de que a informação e os dados (que seriam nada mais do que a forma que essas informações se apresentariam) também seriam bens que necessitariam ser protegidos perante a conduta ilícita nos domínios virtuais. O professor e estudioso Marcelo Xavier de Freitas Crespo[59] , em sua obra, “Crimes digitais”, nega que o bem da informação seja o único bem jurídico penalmente protegido. Seu raciocínio acompanha a lógica da pluri ofensividade e complexidade característica de tais crimes, ao atingir mais de um bem jurídico com sua prática. O professor, lado outro, não chegou a definir quais seriam esses outros bens lesionados.

Contrariando o pensamento jurídico produzido em território nacional, a promulgação da Lei nº 12.737/2012 despertou o entendimento de que o tipo penal 154-A protegeria a privacidade do internauta em seu sentido mais amplo, como afirma o Professor Márcio André Lopes Cavalcante[60] (2013, p. 1), *“o bem jurídico protegido é a privacidade, gênero do qual são espécies a intimidade e a vida privada”.* A doutrina nacional justifica tal tese empregando como argumento a localização topográfica do delito em nosso Código Penal, como se pode perceber:

Código Penal - Parte Especial
TÍTULO I - DOS CRIMES CONTRA A PESSOA
CAPÍTULO VI - DOS CRIMES CONTRA A LIBERDADE INDIVIDUAL
SEÇÃO IV - DOS CRIMES CONTRA A INVIOLABILIDADE DOS SEGREDOS
Art 154-A - Invasão de dispositivo Informático

Deste modo, o crime do Art. 154-A do Código Penal Brasileiro pode ser entendido como um crime contra o indivíduo, em especial contra seu direito básico de liberdade, no tocante à sua privacidade.

---

[59]**CRESPO, Marcelo Xavier de Freitas.** Crimes digitais.
[60]**CAVALCANTE, Márcio André Lopes.** Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. Disponível em: <https://www.dizerodireito.com.br/2012/12/primeiros-comentarios-lei-127372012-que.html>.

Aceitamos o entendimento doutrinário que afirma ser a liberdade individual o bem jurídico resguardado pelo artigo em análise. Quando consideramos, dessa forma, que a liberdade é o bem tutelado, consideramos também que a mesma compreende em si tanto o bem da privacidade, como a proteção à informação. À título exemplificativo, quando consideramos uma invasão à dispositivo informático alheio, com o intuito de obter informações, tem-se, por condição própria da conduta, a lesão à esfera privada de algum sujeito de direitos .

Quando a conduta descrita no caput do Art. 154-A é efetivada, conjecturamos que o espaço particular e privado do sujeito foi invadido. O cunho patrimonial, nessa situação, goza de caráter coadjuvante, pois nem sempre o invasor consegue ter acesso aos dados que busca, nem sabendo inclusive a qual informação ele terá alcance. Se o cibercriminoso, lado outro, tiver acesso à dados em que nada importam para o indivíduo, não há como supor que seria crime patrimonial, pois tal delito só existe quando o bem possui valor para o seu dono, seja pessoal ou econômico.

A proteção ao bem jurídico da honra também não se destaca como principal à conduta do tipo, uma vez que o invasor cibernético pode ter efetuado o delito apenas para provocar aborrecimentos para a vítima, como em hipóteses que envolvem a instalação de vulnerabilidades e de destruição aleatória de dados de um certo sistema.

Como se percebe, entende-se dessa forma que o objetivo do Art. 154-A seria a proteção, em um primeiro plano, à privacidade do internauta, da pessoa possuidora de dispositivo informático. Reitera-se que as condutas elencadas pelo tipo são pluriofensivas, ou seja, lesionam outros bens jurídicos, tais como a informação, o patrimônio, a honra, entre outros, como exposto anteriormente.

Para uma melhor compreensão do delito em estudo, se faz necessária a sua classificação. Primeiramente, cabe dizer que o tipo penal do Art. 154-A se trata de um **crime comum**, podendo ser praticado por qualquer pessoa, ao não exigir que o sujeito ativo goze de certas características para efetivar sua conduta. Também é **crime simples**, pois não encerra dois ou mais tipos em uma só descrição. Também é **crime principal**, pois sua prática não é ligada à conduta de crime anterior, embora possa existir crime prévio à invasão, como por exemplo o estelionato.

O crime de invasão de dispositivo informático também pode ser considerado como **crime formal**, e não como crime material ou de mera conduta, pois não é preciso que sua prática produza o resultado esperado para que seja punida, sendo que as consequências, se efetivadas, se caracterizaram como mero exaurimento. Pode acontecer de, se consumado o crime, haver a incidência de causas de aumento de pena, agravando a mesma, como reza os §§ 2º e 4º do Artigo, ou mesmo pode ocorrer delito mais grave, de acordo com o §3º, também do mesmo artigo 154-A. O crime de invasão também se mostra diferente aos crimes de mera conduta pois não possuem como característica a incidência de um resultado natural. O crime em questão se consuma sem necessitar que resultados específicos ocorram, como acontece com os crimes materiais, por exemplo.

O tipo representa, por isso, um crime de **perigo abstrato**, onde a produção do resultado não é o que se espera, sendo a mesma mero exaurimento da conduta criminalizada. Tal forma legislativa se popularizou diante da atual evolução tecnológica e dos temores que seu uso indevido pode trazer. Assim, segunda importante lição do Professor Bottini[61] :

> "o que caracteriza a sociedade contemporânea não é o maior 'risco' existente, mas a ampliação da 'sensação de risco'. os perigos que afligem a sociedade atual não são maiores do que aqueles que afetavam o cotidiano de nossos avós ou das gerações anteriores – talvez sejam até menores. Mas a 'vivência' destes riscos é mais presente. Seja pelas incertezas científicas sobre as técnicas e produtos que nos são ofertados diariamente, seja pela intensa cobertura feita pela mídia sobre acidentes e catástrofes, há uma sensação de insegurança maior, há um sentimento de proximidade

[61]Disponível em: <http://www.btadvogados.com.br/pt-br/content/crime-de-perigo-abstra- to>.

> do risco. Essa insegurança geral cria um discurso pela antecipação da tutela penal. A sociedade não admite mais aguardar a ocorrência de um resultado lesivo para aplicar uma pena. Há uma política de proibir comportamentos perigosos, mesmo que não causem resultado algum, como consequência desse clamor por maior segurança, maior tranquilidade, frente à nova sensação de riscos."

Dessa forma, entendemos que na sociedade da informação o intuito é sempre a busca pela proteção dos direitos supraindividuais, em uma ação preventiva contra os riscos, e não contra ameaças concretas e materializadas de violação ao bem jurídico tutelado. O legislador vale-se de todos os meios para prevenir e coibir condutas criminosas, fazendo o uso, principalmente, da tipificação de delitos de perigo abstrato. Frente ao Art. 154-A, ora estudado, a simples invasão de dispositivo informático alheio já configura efetivado o crime, independentemente do resultado ao qual o sujeito ativo visava.

O crime em questão também pode ser tratado como **crime de concurso eventual**, pois pode ser cometido por um ou mais agentes. É também **delito instantâneo de efeitos permanentes**, no que diz respeito ao seu caput, na medida em que há exigência de exame de corpo de delito, ao entender que a invasão deixa vestígios. Já as condutas equiparadas, presentes no §1º, seriam consideradas apenas como **crimes instantâneos**, pois não produzem efeito no tempo.

Há também situações onde o crime em questão se caracteriza como **crime putativo**, como quando o sujeito ativo supõe que está praticando alguma conduta típica, como no caso em tela a invasão, mas na verdade a prática não goza de lesividade, como, por exemplo, quando o agente possui autorização para acesso ou quando o dispositivo é completamente desprotegido. O crime de invasão também pode se configurar como **crime impossível**, pela impropriedade do objeto.

Por fim, o crime do caput do Art. 154-A do Código Penal é considerado como **crime próprio de informática**, ou seja, tem como objeto material da prática dados e sistemas próprios do domínio virtual. Já os crimes descritos nos parágrafos

do mesmo artigo, por protegerem também outros bens jurídicos, se caracterizam como **crimes informáticos mistos**.

Pelo crime em questão ser considerado crime comum, o agente ativo poderá ser qualquer pessoa, não se exigindo características em específico. Dessa forma, o tipo não impõe que o sujeito seja, por exemplo, um técnico em informática ou mesmo que trabalhe em serviços que se relacionem ao âmbito cibernético, para praticar o crime de invasão. Nas palavras de MAGGIO[62]: "*O crime de acesso não autorizado é um crime comum, ou seja, pode ser praticado por qualquer pessoa, não sendo necessária qualquer característica ou qualidade pessoal para o efetivo cometimento do delito".*

Importante colocar em voga que não pratica invasão o legítimo usuário que tenha autorização e credenciais para o acesso do dispositivo, mas que mesmo assim obtém dados, os altera ou destrói. Nesse caso, o delito pode constituir crime de dano, de acordo com o Art. 163 do Código Penal, ou até mesmo o crime correspondente à lei nº 9.983/2.000, que estabelece o chamado "peculato informático", específico apenas para os funcionários públicos (Arts. 313-A e 313-B do Código Penal).

O crime de invasão de dispositivo informatico é **crime unissubjetivo**, podendo ser praticado por uma pessoa, admitindo também a coautoria e a participação. A progressão criminosa também deve ser considerada, pois a invasão pode ser verificada como uma pluralidade de práticas delitivas encadeadas por uma sequência causal e uma respectiva unidade de contexto.

Já o sujeito passivo do delito seria a pessoa física ou jurídica que tem a propriedade do dispositivo informático lesionada. Nas lições do Professor CABETTE

---

[62]**MAGGIO, Vicente de Paula Rodrigues.** Novo crime: Invasão… Disponível em: <http://atualidadesdodireito.com.br/vicentemaggio/2012/12/16/invasão-de-dispositivo-informatico-cp-art-154-a>

[63], “qualquer pessoa que tenha sua privacidade violada pelo invasor é sujeito passivo da infração”.

Entende-se que tal rol deve ser ampliado. Atualmente muitos titulares de dados e informações contratam provedores de armazenamento para o serviço de locação e hospedagem de tratamento de dados, por exemplo. Pesquisas[64] realizadas no meio revelam que o Brasil apresenta um percentual de 75% de grandes empresas que já utilizam esse recurso, chamado popularmente de “nuvens”, onde os dados e informações não se encontram hospedados na memória do computador físico da própria empresa, por exemplo, mas são locados em serviços de terceiros. Dessa forma, se o cibercriminoso tiver acesso à esses dados, não terá invadido o dispositivo pertencente ao da empresa, e sim o dispositivo do provedor de armazenamento. Por isso, entende-se que o titular das informações acessadas também necessita de ser protegido, como o é ao final do caput.

Compreende-se que o sujeito passivo também poderá ser o titular dos dados, armazenados em dispositivos informáticos, não sendo necessariamente limitado pela figura do titular do dispositivo em si. Existem situações em que o titular do dispositivo nem mesmo tenha interesse em perseguir criminalmente o invasor de um de seus dispositivos utilizados por clientes, como é o caso de um provedor de armazenamento, que tem um de seus clientes invadidos.

À vista disso, se o titular do dispositivo goza de legitimidade passiva no crime, não seria coerente não atribuir tal legitimidade ao titular dos dados armazenados em dispositivo informático alheio.

---

[63]**CABETTE, Eduardo Luiz Santos**. Primeiras impressões… Disponível em: <http://jus.com.br/revista/texto/23522>.

[64]Disponível em: <http://olhardigital.uol.com.br/noticia/75_das_grandes_empresas_no_brasil_ja_usam_cloud_computing_aponta_estudo/18602>.

O crime em questão se trata de crime doloso, ao exigir que o sujeito ativo realize a conduta de forma voluntária e consciente. O comportamento de invasão não pode ser analisado sem a vontade e objetivo do agente, que seria o interesse em invadir um dispositivo informático.

Pode-se conceber também do dolo eventual, onde o sujeito ativo não queria a produção do resultado, mas assumiu o risco de produzir o mesmo. Por fim, reitera-se que o dolo é a vontade livre e consciente do agente em invadir o dispositivo. Já a expressão "obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita", presente ao final do caput do Art. 154-A, configura um elemento subjetivo do tipo, ou seja, um fim específico de agir que não integra o dolo, apenas ampliando e fundamentando a ilicitude do fato. De acordo com a lição de Bitencourt[65], "Eles especificam o dolo, sem a necessidade de se concretizarem, sendo suficiente que existam no psiquismo do autor".

Destarte, os fins específicos de agir são as elementares do tipo, ao que afirma que, quando o agente pratica a invasão ou seus crimes comparados (Art. 154-A §1º do Código Penal: "*(...) com o intuito de permitir a prática de conduta definida no caput.)* sem gozar das finalidades específicas explicitadas, não pratica o crime dos Artigos 154-A e 154-A §1º do Código Penal.

Já em relação a modalidade culposa do crime em estudo, a mesma inexiste, só se punindo a modalidade dolosa do crime de invasão de dispositivo informático. Em conformidade com o "Princípio da excepcionalidade do crime culposo", normatizado pelo Art. 18, parágrafo único do Código Penal Brasileiro, nenhum indivíduo deverá ser punido por crime senão quando a sua prática se der de forma dolosa. A modalidade culposa, para ser legítima e assim punível no direito penal, necessita de previsão expressa em lei.

---

[65]**BITENCOURT, Cezar Roberto.** Tratado de direito penal: parte geral. Pág. 321 e 322.

A invasão culposa tecnicamente poderá ocorrer, por formas diferentes, porém ela não será punida, como no caso ilustrado por CABETTE[66], onde um técnico de informática contratado para consertar computadores privados acaba excluindo os dados do dispositivo, por imperícia, imprudência ou negligência. Tal conduta, bastante comum, não diz respeito à aplicação de uma sanção penal, podendo ser indenizada, lado outro, em esfera cível. Por não haver tipo culposo da invasão, não há crime.

Na redação do Art. 154-A do Código Penal, o legislador acabou por fazer o uso de muitas expressões que podem assumir diferentes sentidos, o que acaba por prejudicar a interpretação do texto legal. À vista disso, é preciso interpretar o artigo em análise de forma a usufruir de todo o conteúdo que foi produzido. A seguir, o presente trabalho irá examinar, não tendo a pretensão de esgotar o assunto, a estrutura do tipo penal, assim como possíveis interpretações para as expressões que causam dúvida em sua interpretação.

O núcleo do tipo penal examinado é o verbo “invadir”, ou seja, “adentrar” e se “apoderar” de dispositivo informático necessariamente alheio, pois, se assim não o fosse, a simples conduta de invasão não existiria. O termo “invadir” exige, portanto, algo além do que a simples conduta de acesso indevido. É condição crucial do tipo também que o dispositivo em questão seja protegido por mecanismo de segurança, e que o sujeito ativo tenha a intenção de obter, alterar, destruir dados ou informações sem autorização, ou instalar vulnerabilidade com o intuito de obter vantagem ilícita. O crime de invasão se caracteriza como um crime formal que não impõe a produção de certos resultados para a sua consumação, mesmo sendo plenamente possível que esses resultados ocorram.

---

[66]CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/2012… Disponível em: <http://jus.com.br/revista/texto/23522>.

O uso da expressão “invasão” sugere o ‘entrar’, o ‘dominar’, mesmo que de forma mínima, do dispositivo informático de terceiros. Por isso, julga-se infeliz a escolha do legislador ao utilizar tal termo, uma vez que o mesmo não possui uma coerência semântica relacionada à Ciência da Computação. Mais adequado seria a utilização do verbo “acessar”, por exemplo, que pode ser interpretado pela conduta de ler, escrever, obter ou executar dados salvos em dispositivos informáticos. [67]

Outra expressão fundamental e que deixa dúvidas seria a expressão “dispositivo informático”, apresentada no caput do artigo. O mesmo, sem dúvidas, se trata do objeto material da conduta. Ao considerar que o bem jurídico protegido pelo crime de invasão é a privacidade, o que melhor se adequaria como ‘dispositivo informático’ seria apenas os aparelhos eletrônicos que armazenam dados pessoais e íntimos de seu usuário. Como não é de pretensão da lei em estudo estabelecer um rol exemplificativo de quais dispositivos poderiam ser considerados, citamos que, dentre os principais, os celulares e os computadores, estão os Tokens, os Tablets e os GPSs.

Já a expressão “*conectado ou não à rede de computadores”* representa uma expressão ampla, que permite a conexão entre dispositivos de qualquer natureza, conectados à internet, ou não. Na opinião de BITENCOURT, a conexão com a web é irrelevante, pois a “proteção penal não é da rede mundial de computadores, mas da privacidade individual (...)”[68]. Entende-se, por fim, que a intenção de tal expressão foi evidenciar que o delito pode ser praticado tanto através de outro dispositivo, através do uso da internet, como no próprio dispositivo invadido.

A expressão “*mecanismo de segurança”*, por sua vez, representa condição para a prática do delito, pois o legislador só pune a conduta de invadir se a mesma for dirigida a dispositivo protegido. O artigo, porém, não nos estabelece

---

[67]**VIANNA, Túlio Lima.** Fundamentos de direito penal informático (...)
[68]**BITENCOURT, Cezar Roberto.** Invasão de dispositivo informático. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>

quais mecanismos são considerados seguros e se tal proteção é efetiva. A ausência de mecanismo de segurança conduziria à atipicidade da conduta. E a ineficácia desse mecanismo iria assemelhar-se à sua inexistência. O entendimento apresentado, lado outro, não é o majoritário, visto que a doutrina nacional também advoga no sentido de que basta a presença de qualquer mecanismo, não fazendo diferença para a tipificação se o mesmo é efetivo ou não.

Para exemplificar, basta imaginarmos a subtração de um pen drive ou cartão de memória, que não possui nenhum mecanismo de segurança para a proteção dos dados ali armazenados. Se o agente copia esses dados indevidamente e depois os apaga, não há a incidência do crime em estudo, ao entendermos que não há a conduta de "invasão", e sim o simples acesso desprotegido e destruição das informações ali contidas. Poderia o agente responder por crime de dano, previsto no Art. 163 do Código Penal, ou simplesmente responder pelo furto do dispositivo (Art. 155, também do Código Penal).

Expressão primordial também é "*fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou;"* que acaba por trazer à conduta típica formas de exaurimento do crime, pois, como já sabido, o delito se consuma com a invasão. Importante ressaltar que tais efeitos se dão no dolo específico do agente, sendo consumados somente quando não há o consentimento do titular dos dados armazenados.

E, por fim, vale destacar o (fim de) "*instalar vulnerabilidades para obter vantagem ilícita".* Com a inserção de tal conduta no caput do tipo penal, o legislador buscou tipificar conduta posterior à invasão, que seria, no caso, a instalação de vulnerabilidade. Nesse sentido, o entendimento do PL 2.793/2011:

> " *(...) estabelece a necessidade de intenção específica de 'instalar vulnerabilidades, obter vantagem ilícita ou obter ou destruir dados ou informações não autorizados' - ou seja, pune-se apenas quando a conduta*

> *do agente estiver relacionada a determinado resultado danoso ou quando o objetivo do agente for efetivamente censurável (...)"* [69]

A consumação do delito em questão ocorre com a efetiva invasão, constatada por prova pericial digital, que irá fazer uma avaliação dos artefatos e das evidências do ato, como a data e hora de conexão ao dispositivo invadido (login) e a data e hora em que a conexão chegou ao fim (logout). A invasão não pode resultar de presunções, devendo ser comprovada, por pelo menos, uma mínima base probatória.

A doutrina nacional ainda indaga se o delito do Art. 154-A do Código Penal poderia se enquadrar no conceito de **crime permanente**, quando a consumação se prolonga no tempo. Apesar do acesso indevido perdurar por algum período, fato é que com a simples conduta de invasão realizada, consumada está a conduta, ainda que o sujeito se desconecte imediatamente após invadir o dispositivo. O delito se trata, portanto, de espécie de **crime instantâneo**, já que a sua consumação ocorre no momento da invasão, ainda que o sujeito permaneça conectado ao sistema lesionado, pois assim o mesmo não estaria "invadindo" o dispositivo, mas sim apenas acessando um sistema já invadido, já devassado.

No que tange a tentativa, a mesma seria possível, já que o crime em questão se trata de crime plurissubsistente. Segundo o autor e professor CABETTE [70]:

> "É plenamente possível que uma pessoa tente invadir um sistema ou instalar vulnerabilidades e não o consiga por motivos alheios à sua vontade, seja porque é fisicamente impedida, seja porque não consegue, embora tente violar os mecanismos de proteção."

---

[69] **TEIXEIRA, Paulo e outros.** Projeto de lei 2793/2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>.

[70] **CABETTE, Eduardo Luiz Santos.** Crime de invasão de dispositivo informático (artigo 154-A, CP). Disponível em: <https://eduardocabette.jusbrasil.com.br/artigos/153070617/crime-de-invasao-de-dispositivo-informatico-artigo-154-a-cp>.

4.2.2) Crimes Comparados ao de Invasão

Nos termos do §1º do Art. 154-A do Código Penal:

§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.

O núcleo do tipo penal apresentado possui os verbos de *produzir* (gerar, fabricar, gerar resultados), *oferecer* (disponibilizar, proporcionar, expor), *distribuir* (entregar, transmitir, espalhar), *vender* (alienar, comercializar, ceder por certo preço) e *difundir* (transmitir, propagar, disseminar), tendo como objeto material qualquer dispositivo ou programa de computador que tenha o intuito de permitir a invasão de dispositivo informático de terceiros, assim como a prática das mesmas condutas previstas no caput, que seriam as de obter, adulterar ou destruir dados ou informações, ou instalar vulnerabilidades.

O legislador, dessa forma, abrangeu a criação de outro crime, adotando a pena equiparada à da invasão simples. Se caracteriza por ser **crime de ação múltipla** que sanciona o sujeito que provê instrumentos para a prática de invasão. Importante lição de BITENCOURT[71] nesse sentido:

> " *O autor dessas condutas não é autor direto da invasão de dispositivo informático, mas um 'colaborador' sui generis, isto é, expressamente previsto em lei como tal, independentemente de ser alcançado pelo concurso de pessoas, como, normalmente ocorreria, pois pratica condutas declaradamente acessórias, para permitir a execução da invasão. Logicamente, a tipicidade de sua conduta não é abrangida pela norma secundária de ampliação constante do art. 29 do CP, mas decorre do próprio texto legal (154-A §1º).*"

[71]**BITENCOURT, Cezar Roberto.** Invasão de dispositivo informático. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico>.

4.2.3) Figuras Qualificadas

O Art. 154-A §3º, do Código Penal, traz a definição da modalidade equiparada do crime de invasão. O crime é qualificado quando é acrescentada, ao tipo penal simples, alguma circunstância específica que acaba tornando o mesmo mais grave, alterando o mínimo e o máximo das penas cominadas em abstrato. Dessa forma, válida se faz a citação do referido artigo:

§3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Desse jeito, enquanto a modalidade simples ou a equiparada possuem pena de detenção, de no mínimo três meses ao máximo de um ano e multa, as figuras qualificadas, por motivo das circunstâncias específicas, possuem pena de reclusão, de no mínimo seis meses ao máximo de dois anos, e multa. Tais figuras se caracterizam por serem extremamente subsidiárias, pois o legislador, após redigir a sanção penal, exige: “se a conduta não constitui crime mais grave”.

As figuras qualificadas pelo parágrafos são apenas duas, quais sejam:

1) “Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, (...)”.

A figura apresenta, como visto, três hipóteses, a começar pela obtenção de conteúdo (ou apenas o simples conhecimento do assunto, do teor) de comunicações eletrônicas privadas, como por exemplo mensagens advindas de

e-mails, de SMS (da sigla em inglês “Short Messaging Service”), e das mais recentes mensagens do aplicativo “WhatsApp”, por meio dos quais é possível a transferência de mensagens de texto, imagens, vídeos e gravações de áudio, dentre outros. Há também a figura da obtenção de segredos comerciais ou industriais, como por exemplo fórmulas, desenhos industriais e até mesmo estratégias para o lançamento de produtos, e, por fim, temos a figura da obtenção de informações sigilosas, assim definidas em lei, representando assim uma norma penal em branco.

Importante dizer que, tratando de violação de sigilo bancário ou de instituição financeira (Art. 18 da Lei nº 7.492/1986), o crime acaba por ser considerado o mais grave, tendo pena de reclusão, de no mínimo um ano e no máximo quatro anos e multa. Assim, o sujeito responde por esse crime em específico e não pelo delito de invasão de dispositivo informático qualificado.

2) “ *(...) ou o controle remoto não autorizado do dispositivo invadido: (...)”*

Para uma melhor explicação da figura qualificada em questão, temos que levar em consideração que existem hoje em dia diversos programas, chamados de “softwares”, que permitem controlar um dispositivo informático, como um computador, à distância (por meio da internet, por exemplo), fazendo o uso de outro computador ou até mesmo através de um telefone celular, como se o mesmo estivesse a uma mínima distância daquele.

Em linguagem cibernética, o dispositivo informático do agente se denomina “guest”, que significaria “hóspede, convidado”, e o da vítima seria chamado pelo termo de “host”, que quer dizer “hospedeiro, anfitrião”.

A figura qualificada em questão ocorreria quando, logo após a invasão, o agente instala um programa para acesso e controle remoto do dispositivo, sem o consentimento da vítima.

4.2.4) Causas de Aumento de Pena

De acordo com os §§ 2º, 4º e 5º do Art. 154-A do Código Penal, existem duas causas distintas de aumento de pena, incidindo uma delas sobre as figuras simples e equiparada (tipo básico), e a outra, por sua vez, incidindo sobre as figuras qualificadas, como se apresenta a seguir:

Consoante o §2º do Art. 154-A do Código Penal, “Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.” Nessa forma de aumento de pena sobre as figuras simples e equiparada, compreende-se por prejuízo econômico aquele que tem como consequência a perda material ou financeira. Por isso, se o prejuízo resultante gozar de caráter exclusivamente moral, não haverá a incidência da respectiva causa de aumento.

Já o que diz respeito às figuras qualificadas, nos termos do §4º do Art. 154-A do Código Penal, a pena é aumentada de um a dois terços se houver divulgação (ou seja, se houver propagação, dissipação, tornando algo público ou notório), comercialização (alienação, venda) ou transmissão (transferência, difusão) a terceiros, a qualquer título, de informações ou dados conseguidos.

O §5º do referido artigo também integra uma modalidade de aumento de pena em relação às figuras qualificadas. Em seus termos, a pena é aumentada de um terço à metade se o crime for praticado contra o Presidente da República, governadores e prefeitos; contra o Presidente do Supremo Tribunal Federal; contra o

Presidente da Câmara dos Deputados, do Senado Federal, de Assembléia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; e, por fim, contra o Dirigente máximo da administração direta e indireta, federal, estadual, municipal ou do Distrito Federal.

4.3) Lei nº 13.772 de 2018 e o novo crime do Art. 216-B do Código Penal

Em dezembro do ano de 2018 entrou em vigor no País a Lei nº 13.772, que nos apresentou dois propósitos principais: a alteração da Lei nº 11.340, de 7 de agosto de 2006, conhecida como a “Lei Maria da Penha”, para reconhecer que a violação da intimidade da mulher se caracteriza como violência doméstica e familiar, e a modificação do Código Penal, ao introduzir nova conduta típica, qual seja, o ato de registrar, sem autorização, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. O presente estudo irá analisar apenas a mudança apresentada pelo Código Penal Brasileiro e suas implicações no ciberespaço.

Com a rápida evolução dos meios de comunicação e a crescente popularidade dos âmbitos cibernéticos, o Direito Penal, que se caracteriza por ser a *ultima ratio* (último recurso), tem sido acionado de forma constante para defender e proteger certos bens jurídicos que outros ramos do direito não têm conseguido preservar efetivamente. Bens jurídicos como a privacidade, intimidade, liberdade e até informação tem sido lesionados frequentemente, tendo como meio a internet, tornando a conduta mais fácil para os criminosos.

Frente à necessidade de uma regulamentação mais específica, que resguardasse de fato a privacidade do sujeito usuário da rede, o direito penal brasileiro passou a modificar condutas tipificadas já existentes (como se constata a partir da análise da Lei nº 12.735/2012) e a inserir também novos tipos penais no

ordenamento jurídico, como é o caso da neocriminalização das filmagens não consentidas de atos sexuais (atual Art. 216-B do CP).

Por fim, é válida a citação contida no Art. 1º da Lei nº 13.722/2018:

"**Art 1º** Esta Lei reconhece que a violação da intimidade da mulher configura violência doméstica e familiar e criminaliza o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado".

4.3.1) Análise do Art. 216-B do CP

O Art. 3º da Lei nº 13.772/2018 trouxe uma inovação ao Código Penal brasileiro. Foi acrescentado um novo Capítulo, qual seja, o "Capítulo I-A: Da exposição da intimidade sexual), que se encontra dentro do Título dos Crimes contra a dignidade Sexual**.** Dentro deste capítulo é que se encontra a nova conduta tipificada, "registro não autorizado da intimidade sexual", elencada no Art. 216-B do Código Penal:

"**Art. 3º** O Título VI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte Capítulo I-A:

CAPÍTULO I-A:

DA EXPOSIÇÃO DA INTIMIDADE SEXUAL

Registro não autorizado da intimidade sexual

Art. 216-B - Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo."

Oportuno é o entendimento de Rogério Sanches:

> "o tipo preenche a lacuna que existia em relação à punição da conduta de indivíduos que registravam a prática de atos sexuais entre terceiros. Foi grande a repercussão quando, em janeiro de 2018, um casal alugou um apartamento para passar alguns dias no litoral de São Paulo e, depois de se instalar, percebeu uma pequena luz atrás de um espelho que guarnecia o quarto. O inusitado sinal faz com que um deles vistoriasse o espelho e, espantado, descobrisse que ali havia uma câmera instalada. O equipamento foi imediatamente desligado e, logo em seguida, o casal recebeu uma ligação do proprietário do imóvel, que indagou se havia ocorrido algum problema, o que indicava que as imagens estavam sendo transmitidas em tempo real. Embora se tratasse de conduta violadora da intimidade e que inequivocamente dava ensejo a indenização por danos morais, o ato – não tão incomum – de quem instalava um equipamento de gravação nas dependências de um imóvel para captar imagens íntimas sem o consentimento dos ocupantes não se subsumia a nenhum tipo penal. A partir de agora, é classificado como crime contra a dignidade sexual"[72].

Para entender o que o legislador realmente buscou proteger com o crime do novo Art. 216-B, se faz essencial entender o que seria a "exposição da intimidade sexual" e o porque dessa exposição estar intimamente ligada à ideia da ofensa à privacidade do indivíduo.

A palavra "expor" quer dizer "fazer com que fique evidente; colocar à vista; descobrir; retirar as vestes, aquilo que tapa; propiciar o conhecimento de; exibir ou desvelar; fazer com que fique acessível; oferecer; submeter(-se) à

[72] **SANCHES**, 2018, pg. 7.

vergonha; apresentar ao público; colocar em exposição; fazer que todos vejam". [73] Já o conceito de *intimidade* significaria como a "relação estreita ou convívio próximo entre duas ou mais pessoas; privacidade; vida pessoal ou íntima".[74] E o conceito de *sexual* seria definido como tudo *"*relativo a sexo: órgãos sexuais; relação sexual" [75].

Tomando conhecimento dos principais conceitos que integram o delito em questão, chegamos a conclusão de que o ato da exposição da intimidade sexual seria materializado no momento em que o sujeito ativo submete pessoa(s) à vergonha e ao constrangimento. Na prática do artigo em análise, a exposição alcança um menor número de pessoas, visto que o núcleo do tipo se restringe aos verbos de "registrar", "produzir", "fotografar" ou "filmar". Dessa forma, o material elaborado lesiona os direitos fundamentais de privacidade e intimidade do sujeito pelo fato de terceiros adentrarem à esfera tão particular e privada como essa.

Ademais, a conduta pode ser feita através de plataformas digitais, ou seja, o sujeito ativo do crime poderia filmar ou fotografar conteúdo com cena de nudez ou ato sexual ou libidinoso alheio sem consentimento através de aplicativos conectados à web, por exemplo, pelo fato da expressão "*por qualquer meio"*, presente no caput. Assim sendo, além do crime em questão, o sujeito ativo também se enquadraria no Art. 218-C do Código Penal, que será estudado mais adiante, pois o agente, através de tal conduta, acaba por submeter a vítima à uma exposição muito maior, ao transmitir o material em redes sociais, por exemplo.

O Objeto Jurídico que se busca proteger com o delito em questão é a dignidade sexual de qualquer pessoa (Título VI - Dos Crimes Contra a Dignidade Sexual) e, de forma mais específica, a própria exposição dolosa da intimidade sexual de cada indivíduo (Capítulo I-A - Da Exposição da Intimidade Sexual), isto é, o direito de cada sujeito poder dispor da sua própria intimidade sexual. Se a conduta

[73]Disponível em: <https://www.lexico.pt/expor/>.
[74]Disponível em: <https://www.lexico.pt/intimidade/>.
[75]Disponível em: <https://www.lexico.pt/sexual/>.

da exposição criminosa for efetivada, tem-se também a violação do bem jurídico da privacidade e da intimidade da pessoa humana.

Já o Objeto Material do crime em questão seria o conteúdo com cena de nudez e/ou ato sexual ou libidinoso, que goza de caráter íntimo e privado.

O caput do novo artigo do Código Penal brasileiro nos apresenta quatro núcleos: 1) *produzir* (realizar, pôr em prática, gerar resultados) [76], 2) *fotografar* (imprimir a imagem de alguém ou algo por meio de fotos), 3) *filmar* (registrar sequências de imagens por meio de vídeo, gravar, cinematografar) [77] ou 4) *registrar* (alocar, reservar em banco de dados), por qualquer meio (como por exemplo, celulares, câmeras de vídeo, câmeras de computadores, câmeras fotográficas, dentre outras). conteúdo com cenas de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem a autorização e o consentimento dos participantes.

Para uma melhor compreensão do tipo, faz-se importante o entendimento do que se caracterizaria como uma cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Seria, nesta linha, qualquer situação que compreenda uma ou mais pessoas em ambiente privado, particular, não acessível ao público de maneira geral. Certo é que se o ato sexual ocorre em local público, que possibilita o acesso por outras pessoas, o bem jurídico tutelado, que é a intimidade e a privacidade, seria exposto pelo próprio titular, não podendo ser considerado lesionado por terceiros que capturam e registram o momento (SANCHES, 2018, p. 7)[78].

[76]Disponível em: <https://www.sinonimos.com.br/produzir/>.
[77]Disponível em: <https://www.sinonimos.com.br/filmar/>.
[78]Disponível em: <https://s3.meusitejuridico.com.br/2018/12/9c20f715-breves-comentarios-as-leis-13769-18-prisao-domiciliar-13771-18-feminicidio-e-13772-18.pdf>.

Por fim, a intimidade sexual que é deliberativamente exposta pelo agente ou casal em público e/ou lugar exposto, acessível à comunidade, poderá vir caracterizar o crime de ato obsceno, conforme Art. 233 do Código Penal.

É condição crucial e essencial para a existência e configuração do crime do Art. 216-B do Código Penal o não consentimento/não autorização dos indivíduos que participam do ato sexual e/ou libidinoso, por se tratar de um crime que viola o bem jurídico da intimidade.

Se porventura as partes quiserem, deliberadamente, que terceiros filmem, produzam ou fotografem o ato sexual ou libidinoso não haverá tipificado o delito em questão, pois dessa forma a conduta estaria embasada pelo consentimento do então ofendido.

Ainda nesta linha, afirma Rogério Sanches que *"embora a lei utilize a expressão participantes – no plural – não se exclui da incidência do tipo o registro não autorizado de apenas uma pessoa em momento de intimidade*" (SANCHES, 2018, p. 7)[79]. Podemos citar, a título exemplificativo, o namorado que filma, sem consentimento, sua namorada na prática de ato sexual.

O delito analisado é classificado como crime de forma livre, ou seja, o mesmo poderá ser praticado por qualquer meio de execução. O próprio legislador, no referido caput, afirma que a produção, fotografia ou registro pode se dar "*por qualquer meio"*, possibilitando o uso de dispositivos informáticos como o principal meio de execução.

Por se tratar de um crime comum ou geral (crime que pode ser cometido por qualquer pessoa), o tipo penal não exige nenhuma qualidade especial do Sujeito

---

[79]**JÚNIOR, Joaquim Leitão e outros.** COMENTÁRIOS À LEI Nº. 13.772 DE 2018: o novo conceito de violência psicológica da Lei Maria da Penha e o novo delito do art. 216-B do Código Penal Brasileiro. Disponível em: <http://portaljuridicobrasil.com.br/sergiocdreis/coment%C3%A1rios-%C3%A0-lei-n%C2%BA-13772-de-2018-o-novo-conceito-de-viol%C3%AAncia-psicol%C3%B3gica-da-lei>.

Ativo, podendo o mesmo ser qualquer pessoa. O mesmo ocorre com o Sujeito Passivo, podendo ser qualquer indivíduo, desde que seja maior, tendo capacidade de consentir o fato.

O elemento subjetivo do tipo penal é o dolo, seja ele em sua modalidade direta ou eventual, em praticar qualquer das condutas previstas no caput sem o consentimento dos participantes. Não há previsão legal de modalidade culposa, tornando assim impossível a tipificação do crime culposo. Ao final, também não se exige nenhuma finalidade especial por parte do agente ativo, seja financeira ou apenas para satisfazer sua lascívia, por exemplo.

O crime do novo Art. 216-B se consuma com a prática de qualquer uma das condutas representadas no *caput* ou sem seu parágrafo único. Já no que diz respeito à tentativa, a mesma é sim possível, por se tratar de crime plurissubsistente, onde as condutas podem ser fracionadas.

A ação penal respectiva ao caso é a Pública Incondicionada. No caso, se faz crucial salientar que de acordo com o Art. 225 do Código Penal todos os crimes previstos no “Capítulo I e II” são apurados tendo como meio a ação penal pública incondicionada. Porém, o legislador não modificou o Art. 225 com a criação do Capítulo I-A, deixando-o, assim, fora do alcance do dispositivo.

Sabe-se, todavia, que os crimes só serão de ação penal privada ou ação penal pública condicionada se tais modalidades forem expressamente previstas pelo legislador. Por isso, frente à possíveis dúvidas, a conclusão é no sentido de que o artigo analisado se trata de crime de ação penal pública incondicionada, de acordo com o Art. 100 do Código Penal.

É considerado importante, para o presente trabalho, a análise do parágrafo único do aludido artigo. O mesmo afirma que “na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o

fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo".

Como visto anteriormente, os meios tecnológicos presentes na sociedade atual oferecem infinitas possibilidades aos seus usuários. Uma prática que tem se tornado cada dia mais comum, sendo aperfeiçoada por aplicativos e tutoriais cibernéticos, é a famosa "montagem", que pode ser realizada tendo como base fotografias, vídeos ou qualquer outro tipo de mídia.

Em tal caso, não há necessariamente a violação à intimidade e a privacidade do indivíduo, mas sim um constrangimento da imagem da pessoa. [80] Dessa forma, a vítima não participa efetivamente do ato sexual e/ou libidinoso, sendo apenas incluída pelo agente ativo por meio de montagens. Essas mesmas montagens muitas vezes são disseminadas pela Web, expondo a vítima a um infinito número de pessoas, dificultando muitas vezes seu acesso pessoal à internet, pelo imenso constrangimento sofrido.

Na modalidade equiparada, o núcleo do tipo é o verbo *realizar*, que significaria "efetuar, colocar em prática, fazer. Portanto, a ação nuclear indica que o tipo é comissivo, prevendo um comportamento positivo como forma de praticar o delito."[81] Por se caracterizar como um crime plurissubsistente, a tentativa da modalidade em questão é possível e sua consumação se dá com a efetiva montagem sem a autorização da vítima, pouco importando que a mesma seja divulgada ou não (sendo apenas mero exaurimento do tipo penal). O elemento

[80]Há atualmente softwares capazes de simular com muita verossimilhança a participação de alguém em ato sexual praticado por terceiros. Durante as eleições de 2018 foi amplamente divulgado o caso envolvendo um candidato que, segundo se apurou à época, foi vítima deste tipo de conduta, que não encontrava correspondência típica específica, embora pudesse, conforme as circunstâncias, se subsumir à injúria, assim como ocorria com a divulgação de imagens de sexo, nudez ou pornografia, hoje tipificada no art. 218-C do Código Penal. (disponível em: <https://s3.meusitejuridico.com.br/2018/12/9c20f715-breves-comentarios-as-leis-13769-18-prisao-domiciliar-13771-18-feminicidio-e-13772-18.pdf>).

[81]Disponível em: <https://www.estrategiaconcursos.com.br/blog/novo-crime-registro-nao-auto…>.

subjetivo é o dolo, tendo como intuito “incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo”.

Os sujeitos ativos e passivos podem ser praticados por qualquer pessoa. Se a criança ou adolescente for a vítima, ficará configurado o delito do Art. 241-C, do Estatuto da Criança e do Adolescente (ECA). [82]

Finalizando, cita-se que prática também bem comum no âmbito cibernético seria a divulgação de imagens de nudez ou de atos libidinosos de pessoas sósias, ou seja, declaram ser “A”, quando na verdade são “B”. Tais práticas foram popularizadas pelo termo “*fakenews”*, e, apesar de tratar de montagens e suas consequentes violações concernentes à imagem do sujeito, não são abarcadas pelo tipo penal em comento. Tal ato não traz em si montagens em vídeo, fotografia, áudio ou qualquer outra mídia que tenha como objetivo incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. Tal fato, obviamente, não descarta a incidência de outras tipificações legais que se adequem ao caso concreto.

4.3.2) Porque o delito do Art. 216-B pode ser considerado crime cibernético?

Como exposto anteriormente, a conduta tipificada pelo novo artigo do Código Penal Brasileiro, o Art. 216-B, tem como bem jurídico penal protegido a intimidade sexual da vítima. O Art. busca proteger a mesma da exposição indevida de sua nudez ou de seus atos sexuais e/ou libidinosos de caráter íntimo e privado.

---

[82]**Art. 241-C** Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa. Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

Sendo assim, pergunta que se faz pertinente é: “porque o delito do crime 216-B pode ser considerado uma espécie de cibercrime?” E a resposta é simples. O Legislador quis proteger o indivíduo de uma possível exposição de sua intimidade sexual, exposição essa que se dá, praticamente em sua totalidade, através da internet e dos mecanismos da rede.

O delito em estudo apresenta uma forte conexão com a conduta do Art. 154-A, do Código Penal, estudada anteriormente. O sujeito ativo do crime de invasão de dispositivo informático, por sua vez, pode fotografar e filmar terceiros em ato sexual ou libidinoso, sem seu consentimento. Dessa forma, o material íntimo produzido poderia se vincular à web, e teria como meio de produção dispositivos informáticos. A exposição da vítima é inegável, por mais que essa exposição se dê de forma menor do que se comparada com o delito do Art. 218-C, também do Código Penal, que será analisado a seguir.

Dessa maneira, o crime tipificado pelo Art. 216-B pode ser considerado um crime cibernético pelo meio utilizado pelo sujeito, o que muitas vezes reflete na escolha de dispositivos informáticos conectados à internet.

Seguindo a presente linha de raciocínio, se faz extremamente necessário o estudo do Art. 218-C, também do Código Penal Brasileiro, que tipifica a conduta de publicar e divulgar, por exemplo, o material íntimo produzido, principalmente tendo como meio os sistemas de comunicação em massa ou sistema de informática ou telemática.

4.4) Lei nº 13.718 de 2018 e o novo crime do Art. 218-C do Código Penal

Prática bastante comum nos domínios virtuais, principalmente nas populares redes sociais, é a divulgação de cenas de sexo, nudez e até mesmo

estupro. A dissipação de material íntimo se dá sem o consentimento da vítima, que se vê exposta para um número indeterminado de pessoas.

Frente à iminente necessidade de proteção dessas vítimas, que tiveram sua vida sexual exposta na internet, casos que aumentaram consideravelmente nos últimos anos, a Lei nº 13.718/2018 introduziu em nosso Código Penal o novo artigo 218-C, que dispõe sobre os crimes de “divulgação de cena de estupro ou de cena de estupro de vulnerável”, “divulgação de cena com apologia ao estupro” e “divulgação de cena de sexo ou de pornografia”.

Em virtude da complexidade e da extensão do tipo plurisubjetivo, apesar de apresentar muitos pontos em comum, se faz possível a constatação da existência de três crimes diferentes: o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, o crime de divulgação de cena com apologia ao estupro e o crime de divulgação de cena de sexo ou pornografia.

Como se pode perceber, o núcleo do tipo se perfaz no verbo “divulgar”, ou seja, “tornar pública (alguma coisa desconhecida por outrem); propagar, publicar; promover-se, fazendo-se conhecer”.[83]

É através de plataformas digitais, conectadas à rede mundial de computadores, que os cibercriminosos costumam expor e dissipar imagens, fotos e registros de pessoas que se encontram em cenas de nudez ou ato sexual ou libidinoso, de caráter íntimo e privado. Dessa maneira, o agente ativo do crime submete a vítima à vergonha e ao intenso constrangimento, expondo a vida privada sexual da mesma para um infinito número de pessoas, as quais acabam por ter

[83]Dicionário Google. Disponível em: <https://www.google.com/search?q=significado+de+divulgar&oq=significado+de+divulgar&aqs=chrome..69i57.4403j0j7&sourceid=chrome&ie=UTF-8>.

acesso à informações privadas relativas aos seus órgãos e relações sexuais, por exemplo.

Dessa maneira, o crime do Art. 218-C se torna um crime cibernético pelo meio de execução escolhido pelo sujeito ativo. Aquele que divulga fotografias, vídeos ou outro registro audiovisual, que gozam de caráter íntimo e privado, sem autorização e consentimento, acaba por escolher a internet para expor a vítima.

Muito importante colocar em voga o fato de que a vítima quase sempre também é usuária da web, e por isso, além de sofrer inúmeros abalos psicológicos, muitas vezes irreparáveis, tem a sua privacidade extremamente lesionada prejudicando o seu acesso e uso do âmbito informático.

4.4.1) Análise do Tipo Penal

Divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia

Art. 218-C Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia:

Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.

Aumento de pena:

§ 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

Exclusão de ilicitude

§ 2º Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos."

O bem jurídico tutelado pelos crimes do Art. 218-C é o bem da dignidade sexual da vítima, que é lesionada pela divulgação sem autorização das imagens e vídeos íntimos e privados. A privacidade e a intimidade também são fortemente violados pela conduta efetiva da divulgação, ofendendo também o Princípio da Dignidade Humana.

Já o Objeto Material do crime ora analisado seria o conteúdo dissipado com cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou cena de sexo, nudez ou pornografia, que gozam de caráter íntimo e privado.

O caput do novo artigo penal possui como verbos o "*oferecer"* (expor, exibir, abastecer, propor que seja aceito), "*trocar"* (permutar, comutar, mutuar)[84], "*disponibilizar*" (tornar disponível, acessível, viabilizar, possibilitar)[85], "*transmitir*" (propagar, difundir, disseminar, divulgar)[86], "*vender"* (alienar por certo preço, comercializar, transferir)[87] ou "*expor à venda*" (apresentar, colocar à mostra para alienação, expor para comercialização, fazer propaganda), "*distribuir"* (entregar a

[84]Disponível em: <https://www.sinonimos.com.br/trocar-2/>.
[85]Disponível em: <https://www.sinonimos.com.br/disponibilizar/>.
[86]Disponível em: <https://www.sinonimos.com.br/propagar/>.
[87]Disponível em: <https://www.sinonimos.com.br/vender/>.

várias pessoas, espalhar, difundir, partilhar)[88] ou "*divulgar"* (tornar público, conhecido, popularizar, revelar, externizar)[89] por qualquer meio, inclusive por meio de comunicação em massa ou sistema de informática ou telemática, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro (Art. 213 do Código Penal), que contenha cena de estupro de vulnerável (Art. 217-A do Código Penal), que faça apologia de estuprador ou estuprador de vulnerável, que induza a prática de estupro ou de estupro de vulnerável, e, por fim, que contenha cena de sexo, nudez ou pornografia, **sem o consentimento da vítima**.

O crime do Art. 218-C do Código Penal se configura como um **crime comum**, e, por isso, qualquer pessoa pode ser sujeito ativo do delito. Quer dizer que o indivíduo não deverá apresentar nenhuma característica em específico para se tornar apto à prática do crime.

Na hipótese de divulgação de cena de estupro ou de cena de estupro de vulnerável não é necessário que o sujeito ativo seja pessoa que participa ativamente do delito. Da mesma forma ocorre no crime de divulgação de cena de sexo ou pornografia, não se faz necessário que o agente seja pessoa que mantenha ou tenha mantido relação de cunho íntimo e sexual com a vítima, podendo ser qualquer pessoa.

Ademais, caso o delito seja praticado por indivíduo que mantém ou que tenha mantido relação íntima de afeto e carinho com a vítima, a pena será aumentada, conforme os termos do §1º do Art. 218-C da legislação penal. Apenas nessa hipótese, será exigida uma especial qualidade do agente.

O sujeito passivo, por sua vez, também pode ser qualquer pessoa. A vítima deverá ser maior de 18 (dezoito) anos, pois, caso a mesma seja menor de

[88]Disponível em: <https://www.sinonimos.com.br/distribuir/>.
[89]Disponível em: <https://www.sinonimos.com.br/divulgar/>.

idade, irá incidir o crime dos Arts. 241 e 241-A do ECA (Estatuto da Criança e do Adolescente).

Os verbos que estão presentes no núcleo do tipo são os verbos "*oferecer"*, que significa apresentar para a aceitação ou rejeição, proporcionar algo; "trocar", que caracterizaria a conduta de dar e receber concomitantemente; realizar permuta; "disponibilizar", que expressa a prática de oferecer, dispôr, colocar à disposição; "transmitir", ou seja, fazer passar de um local para outro, divulgar, publicar algo; "vender" que seria a prática de alienação mediante pagamento pecuniário, ou expor à venda; "distribuir", que pode ser considerado como a conduta que divide algo entre duas ou mais pessoas; "publicar", que seria o ato de tornar público, visível e conhecível ao público; e "divulgar", que é o ato de difundir, disseminar e propagar algo.

O ato de divulgar, em ambos os casos suscitados pela lei, poderá ocorrer por qualquer meio, principalmente por meio de comunicação de massa, por meio de sistemas de informática ou telemática, vídeo, fotografia ou outra mídia. Os meios de comunicação em massa, o qual o caput do artigo se refere, pode ser entendido como a vinculação de mensagens a um número de pessoas simultaneamente, como ocorre, por exemplo, com as mídias habituais, como as emissoras de televisão, as revistas e os jornais.

Já os sistemas informáticos, por sua vez, caracterizam um conjunto de sistemas organizados, os chamados "*softwares*", juntamente com equipamentos, os "*hardwares*", que são embasados por circuitos eletrônicos capazes de manejar, transformar e transmitir informações através de dados, tendo como meio a rede mundial de computadores, por exemplo.

Os sistemas telemáticos, expressão também utilizada pelo legislador na redação do artigo, são compreendidos como qualquer meio que possa realizar a transferência de dados através do uso associado entre sistema computacional e sistemas de telecomunicação, como ocorre com os telefones, as redes móveis e os famosos e populares aplicativos de smartphones, como o *Whatsapp* e o *Telegram*, por exemplo. Desta feita, pode-se perceber como foi importante para o cenário social e cultural atual que o legislador incluísse tal expressão no artigo ora analisado, pois a conduta de divulgação de imagens íntimas e afins tem como principal meio de vinculação tais aplicativos.

Vale também, para nosso estudo, a análise do objeto material da conduta. A "fotografia", indicada pelo caput, nos é entendida como a imagem estática obtida por meio de máquinas fotográficas, sejam as mesmas digitais ou analógicas, de celulares ou de qualquer outro dispositivo informático. Já a mídia que é entendida como "vídeo" seria aquele conjunto alinhado e sequencial de imagens, que, juntas, formariam movimentação. O "outro registro audiovisual", contido no caput do Art. 218-C, seria qualquer outra forma de se registrar áudio e imagens, sequenciais ou não, tendo, como exemplo, os populares "*gifs"* e os "*slides*".

A divulgação também poderá ocorrer por qualquer outro meio, sendo o mais comum o digital, nada impedindo que o sujeito ativo utilize de meio físico para tanto, como ocorre com a impressão de imagens.

Questão polêmica em nosso estudo seria a que tange à divulgação de apenas áudio com cunho sexual. Entende-se, dessa forma, que a divulgação de gravação de voz, sem vinculação à imagem, não configuraria o crime em questão, já que o tipo penal exige que o registro feito seja, ao menos, visual ou audiovisual, ou

seja, que contenha apenas imagem ou imagens e sons, sendo a imagem figura fundamental, não se aplicando, por óbvio, quando apenas há o registro de áudio.

Mediante às considerações gerais feitas, que pertencem à caracterização dos três crimes abordados, passa-se à análise dos elementos específicos de cada um deles.

A primeira divulgação que o tipo penal aborda diz respeito à **divulgação de cena de estupro ou de cena de estupro de vulnerável**. Cena de estupro é aquela em que, mediante qualquer mídia visual ou audiovisual, retrata o constrangimento de alguém, mediante violência ou grave ameaça, a realizar conjunção carnal ou a praticar ou permitir que se pratique qualquer outro ato libidinoso. Já a cena de estupro de vulnerável é a retratada, através de qualquer meio visual ou audiovisual, de prática de conjunção carnal, ou outro ato libidinoso, contra pessoa menor de 14 (catorze) anos de idade, debilitada ou que tenha algum tipo de deficiência mental.

Importante salientar que caso a vítima que é mostrada na cena divulgada seja pessoa menor de 14 (catorze) anos, irá incidir o crime tipificado pelo Art. 241 ou o crime do Art. 241-A, ambos do ECA (Estatuto da Criança e do Adolescente), que possui uma pena mais elevada, e, por isso, mais grave.

Finalmente, se a cena divulgada apresentar crime de violação sexual mediante fraude, tipificado pelo Art. 215 do Código Penal, de assédio sexual, consoante ao Art. 216-A, também do Código Penal, ou de qualquer outro delito que atente ao bem da dignidade sexual que não seja caracterizado pelo estupro ou estupro de vulnerável, o fato será caracterizado como a conduta do Art. 154-A do

Código Penal, caso, obviamente, estejam presentes os requisitos para a tipificação deste.

A segunda divulgação tratada pelo Art. 218-C do Código Penal é a **divulgação de cena com apologia ao estupro**. Tal crime pune o indivíduo que, de qualquer forma, incentiva e induz a prática do crime de estupro. Não é necessário, no momento de induzir e incitar a prática, que exista cena de cunho sexual ou pornográfico, bastando apenas a argumentação e a simples apologia nesse sentido. Caso recente e famoso que pode ser utilizado como exemplo é o caso do conhecido "youtuber Everson Zóio", no qual o mesmo confessa e se glorifica em vídeo pela prática de um estupro.

Questão controvertível é aquela que diz respeito ao chamado "estupro encenado", que seriam vídeos produzidos de forma deliberada, encenando cenas de estupro. O intuito de tal encenação seria a satisfação da lascívia daqueles que assistem a cena. O presente trabalho apresenta entendimento positivo no sentido da conduta descrita caracterizar o crime de divulgação de cena com apologia ao estupro.

Por fim, considerando o tipo de divulgação mais pertinente e adequada ao conteúdo estudado pela presente obra, há a **divulgação de cena de sexo ou de pornografia**. O crime em questão pune aquele sujeito que dissipa para um número indeterminado de pessoas **cena de sexo**, que é considerada como o vídeo ou foto que contenha, explicitamente, a prática de coito ou qualquer outra forma de conjunção carnal; **nudez** e **pornografia**, que é a mídia em forma de figura, fotografia ou filme que busca provocar erotismo obsceno, assim como causar excitação

sexual, não gozando de nenhum valor artístico. Importante ressaltar que nenhuma dessas mídias é produzida com o consentimento da vítima.

Enfim, há de se ressaltar que, segundo Matheus Falivene de Sousa:

> "a divulgação de vídeos e imagens 'profissionais', oriundos de produtoras de vídeo ou de revistas que contenha cena de sexo ou de pornografia sem a autorização das vítimas, não configura o crime em comento, mas sim crime contra a propriedade imaterial"[90].

Os crimes tipificados pelo Art. 218-C do Código Penal possuem modalidade essencialmente dolosa, ao exigir que o agente tenha ciência do compartilhamento ou da divulgação da fotografia, do vídeo ou de qualquer outro conteúdo que compreenda cena de estupro, que incentive a realização de tal prática ou que contenha cena de nudez, sexo ou pornografia que não tenha autorização da vítima.

Para que haja a consumação do crime, o sujeito ativo precisa ter certeza de que o conteúdo dissipado se trata de cena de estupro, de apologia ao estupro, ou de nudez, sexo ou pornagrafia sem a autorização do sujeito passivo, não se admitindo, dessa forma, o dolo eventual.

Se trata de **crime formal**, também chamado de crime de "consumação antecipada", por não exigir a produção de qualquer resultado naturalístico para efetivar a conduta. Geralmente, os núcleos do tipo analisado são instantâneos, se consumando no preciso momento em que a conduta é praticada. Lado outro, as condutas representadas pelos verbos "*oferecer, disponibilizar, divulgar e expor à venda"* podem vir a configurar espécies de crime permanente, sendo comportável, a essas situações, a prisão em flagrante.

---

[90]**SOUSA, Matheus Herren Falivene de.** Comentário ao Art. 218-C do Código Penal. Disponível em: <https://matheusfalivene.jusbrasil.com.br/artigos/630364992/comentario-ao-art-218-c-do-codigo-penal>.

Válida é a constatação que não é proibida a divulgação de toda e qualquer forma de material pornográfico produzido, ao passo que, os vídeos comerciais elaborados por produtoras do gênero contam com consentimento presumido e até mesmo contratual.

Percebe-se, por fim, que em casos de aumento de pena com o fim de vingança ou humilhação, os chamados casos de “pornografia de vingança”, há o elemento subjetivo do tipo, ou seja, o dolo específico de se retaliar a vítima lhe causando extrema humilhação, violando sua privacidade e intimidade.

No que diz respeito à modalidade tentada, por se tratar de crime plurissubsistente, onde a prática pode ser perfeitamente fracionada, é admissível sim o “*conatus”*, ou seja, a tentativa. Ocorre quando o sujeito ativo, por circunstâncias alheias à sua vontade, não consegue consumar o crime.

De acordo com o § 1º do Art. 218-C do Código Penal, a pena é aumentada de um terço a dois terços se o crime for praticado por agente que mantém ou que tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação.

A primeira situação apresentada diz respeito à divulgação por sujeito ativo que mantém ou que manteve relação íntima de afeto com a vítima, ou seja, que tenha ou teve com a mesma um relacionamento amoroso, afetivo e/ou íntimo, ainda que não tenha ocorrido a prática de ato sexual anterior. Por isso, o aumento de pena pode incidir sobre a figura dos cônjuges, companheiros (as), namorados (as) e amantes, assim como qualquer outra pessoa que mantenha relação íntima de afeto e estima, independente da denominação que recebe ou a condição em que se encontra.

Já a segunda hipótese refere-se à conduta conhecida como *"revenge porn",* ou seja, a pornografia por vingança, que busca a divulgação de material íntimo com o intuito de humilhação e intenso constrangimento. Muitas vezes impulsionados por sentimentos como ciúmes e rejeição, por exemplo, os sujeitos ativos do crime divulgam materiais como "*sex tapes*" ou "*nudes*" na internet. Em tal caso, se faz necessária a efetiva demonstração do elemento subjetivo de dolo específico, que consiste no fim particular de vingança. Qualquer outro intuito pertencente à divulgação não acarretará a incidência da causa de aumento de pena.

Já no que tange à pornografia que tem como fim específico a humilhação, também se faz necessário a demonstração do dolo específico, que se caracteriza no objetivo especial de humilhação. Qualquer outro intuito que possa vir a ter a conduta de divulgação não causará a incidência do aumento de pena.

De acordo com a previsão do §2º do Art. 218-C do Código Penal, não há crime quando o agente pratica as condutas descritas no *caput* do artigo em publicação que goze de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua autorização prévia, caso seja maior de 18 (dezoito) anos.

Isto posto, o próprio tipo penal acaba por prever uma causa de exclusão de ilicitude, admissível em situações em que a cena de estupro ou em que as cenas pronográficas são publicadas através de mídias jornalísticas, como a publicação que goza de natureza informativa em mídias tradicionais ou sociais, como o "*facebook"* e o "*instagram"*; quando a publicação dessas mesmas cenas se der de forma científica, ou seja, relativa ao estudo e à análise de específico ramo da ciência humana; ou quando tiver caráter cultural, no que tange ao desenvolvimento artístico. Por fim, as publicações desse conteúdo que tiverem fins acadêmicos, como os

relativos às pesquisas, aulas e palestras, por exemplo, também irão fazer o uso da exclusão de ilicitude.

Todavia, para que a exclusão de ilicitude incida sobre o caso se faz necessário que a vítima seja maior de 18 (dezoito) anos, e que autorize de forma expressa a publicação, se adotando, ainda, recurso que dificulte a sua identificação para com o público. Por isso, é essencial, a priori, que a vítima seja maior de 18 (dezoito) anos, pois, se for o caso em que a mesma seja menor de idade, restarão tipificados os crimes de Divulgação de pornografia infantil, consoante os Arts. 241 e 241-A, ambos do ECA (Estatuto da Criança e do Adolescente).

A pena cominada para o crime do Art. 218-C do Código Penal é a reclusão, que possui o mínimo de 1 (um) a 5 (cinco) anos, se o fato não constituir crime mais grave. A ação penal é pública incondicionada. Na modalidade prevista no *caput*, é admissível a suspensão condicional do processo, nos moldes do Art. 89 da Lei nº 9.099/1995.

4.4.2) Vazamento de Imagens Íntimas na Internet

Os casos que envolvem o vazamento de imagens íntimas, apelidado popularmente como “nudes”, sem o consentimento das pessoas que aparecem nas imagens, ganham cada vez mais espaço, aumentando consideravelmente o número de ocorridos. É o que nos afirma o delegado titular da Delegacia de Repressão ao Crimes de Informática (DCRI), do Rio de Janeiro, Alessandro Thiers [91].

[91]Declaração dada em entrevista concedida ao Portal G1. Diponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado.html>.

Segundo o delegado:

> "Em primeiro lugar, com ampla vantagem, nós temos os crimes de vazamento de fotos e vídeos íntimos, com pessoas ofendidas na sua honra. Depois, temos a pedofilia, que as pessoas infelizmente botam bastante na internet. Em terceiro lugar, temos as fraudes financeiras, de uma forma geral. Em quarto lugar, nós temos os crimes de apologia: a atos criminosos, homofobia, racismo, intolerância religiosa" [92].

Dados fornecidos pela ONG Safernet, a entidade responsável por acompanhar e controlar crimes e violações dos direitos humanos na internet, demonstram que no ano de 2014 foi registrado o maior número de casos de vazamento e disseminação de fotos e vídeos íntimos sem a autorização das vítimas expostas. No mesmo ano, a ONG recebeu a notificação de 224 casos do tipo, contra, por exemplo, apenas 101 em 2013. Os números correspondem apenas ao âmbito brasileiro.

Ainda segundo o delegado Alessandro Thiers, as mulheres são as principais vítimas dos vazamentos de fotos e vídeos íntimos no País, principalmente no estado do Rio de Janeiro. A conduta, chamada de "pornografia de vingança", objetiva exatamente provocar humilhação e constrangimento, ao expor material íntimo da vítima na internet. Há dolo em ofender a privacidade e a intimidade da mesma, dificultando sua vida, principalmente no ambiente social informático.

As análises realizadas pela ONG Safernet comprovam a popularidade da conduta em questão. Os chamados casos de *"sexting"* (que seria a divulgação de conteúdos eróticos por meio da internet, através de computadores e "*smartphones*") podem ser considerados até mesmo como um problema de gênero.

---

[92]Alessandro Thiers. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado.html>.

Apesar de homens e mulheres compartilharem imagens íntimas, são as mulheres que mais sofrem com o vazamento de imagens íntimas, representando 81% do total das vítimas. Os homens representam apenas 16% das queixas e 3% das vítimas não têm seu gênero identificado.

As principais vítimas não apenas são do sexo feminino, assim como são jovens. De acordo ainda com as estatísticas fornecidas pela ONG, cerca de 53% dessas vítimas têm menos de 25 anos de idade. Destas, 25% são menores, tendo idade entre 12 e 17 anos. Já os estados de São Paulo, Rio de Janeiro e Minas Gerais configuram no topo de incidência de tal crime.

De acordo com a coordenadora psicossocial da ONG Safernet, Juliana Cunha, o sentimento de culpa nas vítimas costuma ser comum. Na fala da mesma: “Geralmente as vítimas sofrem com muitos transtornos, mentais, físicos e psicológicos”. [93]

Com o advento da popularização dos “*smartphones”* e de seus aplicativos, a conduta de vazamento de fotos íntimas pela internet aumentou consideravelmente nos últimos anos. Ainda segundo pesquisa realizada pela Safernet, antes de 2012 tais imagens eram mais frequentemente disseminadas em redes socias, como o extinto “*orkut*” e o atualizado “*facebook*”. Os aplicativos, por sua vez, facilitaram as vias de comunicação.Programas como o “*Whatssap”* e o “*Instagram*”, que estão a um clique de acesso, fizeram aumentar os casos que envolvem pornografia de vingança, além de propiciar o acesso à tais imagens para um maior número de pessoas, talvez até indefinidamente.

Por fim, um dos principais problemas ressaltados pela Safernet é a dificuldade das vítimas em apagar os registros na internet das imagens vazadas sem

[93]Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado.html>.

seu consentimento. O marco civil e as Leis nº 12.735 e nº 12.737, ambas de 2012, realmente configuraram um grande avanço no combate aos crimes cibernéticos. Porém não tratam de condutas específicas, como a presente questão. O máximo que as vítimas tinham ao seu dispor estava presente no Artigo 21 do Marco Civil da internet, a lei nº 12.965/2014, que garantia o direito ao esquecimento.

Portanto, através do novos arts. 216-B e 218-C, ambos do Código Penal, tem-se uma efetiva proteção à vítimas que foram por essa obra analisadas. Os artigos reconhecem a presente realidade dos usuários da internet e suas tecnologias, assim como os riscos que o uso da web nos proporciona. Condutas específicas e especiais como as tratadas necessitavam de uma tipificação própria, pois não eram abrangida antes com nossas leis penais, extremamente genéricas.

4.4.3) Caso Neymar e sua adequação ao Tipo 218-C do Código Penal

Para destacar ainda mais a incidência e recorrência do crime ora estudado, se fez conveniente, à título de exemplificação, nos pronunciarmos sobre o atual caso do Jogador de futebol brasileiro Neymar da Silva Santos Júnior, um dos esportistas mais conhecidos no mundo. No dia 15 (quinze) de maio de 2019, foi registrada em uma delegacia de São Paulo uma acusação de estupro contra o jogador. No boletim de Ocorrência, a autora da denúncia declarou que sofreu um estupro, no quarto em que estava hospedada, no Hotel chamado Sofitel Paris Arc Du Triomphe, em Paris, na França. A vítima ainda relatou que estava profundamente abalada, e por isso só registrou a denúncia na cidade onde reside, em São Paulo.

Como o caso ganhou repercussão mundial, sendo um dos assuntos mais tratados pela mídia, Neymar chegou a publicar em suas redes sociais um vídeo onde o mesmo tentava se defender. O arquivo publicado pelo jogador ultrapassou a marca de 18 milhões de visualizações em apenas um dia, mas acabou por ser

excluído pela própria rede social na manhã do dia seguinte. De acordo com o aplicativo “Instagram”, a rede social utilizada por Neymar, a divulgação as mensagens e fotos íntimas violava a política de privacidade da rede.

O jogador então, sob o pretexto de se defender e apresentar a sua versão do ocorrido, publicou conteúdo de cunho sexual, relacionado à nudez e/ou pornografia, sem autorização para tanto. Desse modo, Neymar deu visibilidade a matéria que é enquadrada como conduta típica do Art. 218-C do Código Penal. Os policiais da Delegacia de Repressão aos Crimes de Informática (da sigla DRCI) já intimaram Neymar e já se pronunciaram quanto ao caso nos meios de comunicação.

De acordo com o advogado criminal especialista em direito digital e cibercrimes, José Colhado, “*Não é dessa forma que se faz prova processual. É nos autos e não tornando isso público”*. Consoante com o especialista, mesmo que a acusação de estupro seja falsa, o jogador não deveria, em hipótese alguma, recorrer a uma defesa que possa ser classificada como a prática de outro crime. O gesto mais arrazoado e conveniente, segundo o advogado, seria o jogador comunicar a seu público a existência de conversas e imagens que aparentemente comprovariam a sua inocência, encaminhando as aludidas provas diretamente à Justiça. Se assim o jogador procedesse, iria efetivar seu direito à defesa de forma a não lesionar nenhum outro direito da vítima, como o fez, ao violar a privacidade e a intimidade da vítima que se viu exposta a um intenso constrangimento.

O Artigo 218-C do Código Penal Brasileiro está vigente desde setembro de 2018, e prevê pena de um a cinco anos de reclusão ao sujeito que oferece, troca, disponibiliza, transmite, vende ou expõe à venda, distribui, publica ou divulga, por

qualquer meio - inclusive é destacado no *caput* os meios de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que tenha como conteúdo cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia. Como se pode perceber, há o perfeito enquadramento do tipo penal com a conduta realizada pelo jogador de futebol.

De acordo com Ricardo Caiado, advogado e especialista em direito penal empresarial, compliance e investigações, antes da vigência do art. 218-C do Código Penal, o comportamento em questão era *“enquadrado em crimes contra a honra, como difamação, calúnia e injúria”*. O advogado afirma que a criação desse novo tipo penal seguiu o propósito de coibir a divulgação e dissipação de cenas íntimas em ambiente digital, conduta extremamente lesiva que se tornou recorrente no domínio tecnológico. Ricardo Gaiado ainda afirma: *“Deve haver cautela, não apenas no caso do Neymar. Qualquer conteúdo publicado deve ser muito bem calculado para evitar uma alegação de violação de intimidade".*

5) Conclusões

Diante do estudo apresentado, pode-se tecer as conclusões de que é inegável que a tecnologia e os novos meios de comunicação estão incorporados ao cotidiano, gozando de essencialidade para o desenvolvimento do mundo moderno e para a evolução da humanidade. Dessa forma, o âmbito digital e suas tecnologias implicam em uma rápida comunicação, favorecendo o desenvolvimento econômico, social e cultural.

Lado outro, essa rápida circulação de informações traz consigo um grande risco à privacidade, à intimidade e à vida das pessoas. O domínio digital e o fácil acesso à suas tecnologias propiciam um ambiente favorável para a prática de novos crimes, os chamados “crimes próprios de informática”, conhecidos também como os “crimes cibernéticos” ou “crimes digitais”. O compartilhamento indevido de dados pessoais, feito sem consentimento e com o intuito de prejudicar alguém, pode trazer consequências irreparáveis e imensuráveis para a vítima.

A experiência que já tivemos com a intensa banalização dos avanços tecnológicos nos demonstram que direitos fundamentais à pessoa e à sua dignidade humana são constantemente violados. Por isso, a elaboração do presente estudo se propôs a contextualizar os cibercrimes, para posteriormente analisar as principais fontes legislativas penais, criadas em nosso ordenamento, que buscam combater os cibercrimes, e se as mesmas efetivaram seu mister de proteger efetivamente os direitos básicos lesionados, principalmente no que tange a privacidade do indivíduo.

Entende-se que as novas práticas tipificadas pelo Art. 154-A da Lei nº 12.737/2012 buscam sim a proteção do bem jurídico da privacidade, tendo como objeto material a informática. O legislador buscou, em sua redação, resumir em um único tipo penal o conteúdo produzido pela “Convenção de Budapeste”. Ocorre,

entretanto, que o legislador acabou por produzir um tipo penal atécnico, fazendo o uso de expressões dúbias ao provocar muitas dúvidas em sua aplicação. Ademais, práticas comuns no ambiente digital, como a produção e divulgação de fotos íntimas na internet, sem a autorização da vítima, não eram abrangidas pelo tipo, pelo fato do mesmo ter se limitado apenas à conduta de invasão à dispositivo informático alheio, mediante, ainda, à violação de mecanismo de segurança.

Á vista disso, percebe-se que estávamos tratando, de forma negligenciada, situações que expõem a vida privada do sujeito, que lida com danos irreparáveis à sua privacidade, podendo causar consequências desmedidas, como o rompimento de um matrimônio, indo até mesmo ao suicídio.

Desta monta, a criação dos novos artigos do Código Penal, os arts. 216-B e 218-C, apesar de terem como objetividade jurídica o bem da dignidade sexual, protegem de forma efetiva a privacidade da pessoa humana, ao criminalizarem práticas que antes não eram concebidas em nosso sistema penal. Tais crimes, por sua vez, não se caracterizam como **crimes próprios de informática**, como o tratado no Art. 154-A do Código Penal, mas se fizeram essenciais ao ambiente digital, pois o principal **meio** utilizado para a prática desses novos artigos é a internet e seus mecanismos tecnológicos.

Para finalizar a presente obra, vale destacar que a nossa legislação penal digital ainda se encontra em evolução, se adaptando ao novo cenário que se forma através da progressão contínua da tecnologia. Com o passar do tempo, teremos mais necessidades específicas, advindas de condutas exclusivamente digitais, assim como de condutas que utilizam como meio de realização a internet e suas tecnologias.

Após contextualizar os crimes cibernéticos e analisar os Arts. 154-A, 216-B e 218-C, todos do Código Penal Brasileiro, se dá por concluído o presente

trabalho, com a gratidão pela iniciativa de nosso Ordenamento Jurídico atuar em nova e comprometedora área, a do Direito Informático.

6) Referências bibliográficas

Agência Brasil. Brasil é o 4º país em número de usuários de internet. Disponível em: <https://exame.abril.com.br/tecnologia/brasil-e-o-4o-pais-em-numero-de-usuarios-de-internet/>. Acesso em: 22 abr. 2019.

ANDREUCCI, Ricardo Antônio. O NOVO CRIME DE REGISTRO NÃO AUTORIZADO DA INTIMIDADE SEXUAL. Disponível em: <https://emporiododireito.com.br/leitura/o-novo-crime-de-registro-nao-autorizado-da-intimidade-sexual>. Acesso em: 29 abr. 2019.

BITENCOURT, Cezar Roberto. Invasão de dispositivo informático. Atualidades do Direito, 7 fev. 2013. Disponível em: <http://atualidadesdodireito.com.br/cezarbitencourt/2012/12/17/invasao-de-dispositivo-informatico/>. Acesso em: 14 mai. 2019.

BOECKEL, Cristina; COELHO Henrique. Vazamento de 'nudes' é crime virtual mais comum no Rio, diz delegado. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2015/11/vazamento-de-nudes-e-crime-virtual-mais-comum-no-rio-diz-delegado.html>. Acesso em: 15 abr. 2019.

BRITO, Auriney. Direito penal informático / Auriney Brito. — São Paulo : Saraiva, 2013.

CABETTE, Eduardo Luiz Santos. Primeiras impressões sobre a Lei nº 12.737/12 e o crime de invasão de dispositivo informático. Jus Navegandi, Teresina, ano 18, n° 34936, 23 jan. 2013. Disponível em: <http://jus.com.br/revista/texto/23522>. Acesso em: 16. mai. 2019.

CASTRO, Rodrigo. ENTENDA O CASO: NEYMAR E A ACUSAÇÃO DE ESTUPRO. Disponível em: <https://epoca.globo.com/entenda-caso-neymar-a-acusacao-de-estupro-23715005>. Acesso em: 03 jun. 2019.

FRABASILE, Daniela. Empresas no Brasil estão entre as mais vulneráveis a ciberataques, diz estudo da IBM. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/07/custo-com-violacao-de-dados-no-brasil-e-o-menor-do-mundo.html>. Acesso em: 29 abr. 2019.

GOMES, Helton Simões. Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml>. Acesso em: 22 abr. 2019.

JESUS, Damásio de. Manual de crimes informáticos / Damásio de Jesus, José Antonio Milagre. – São Paulo : Saraiva, 2016.

JÚNIOR, Joaquim Leitão. As Inovações Legislativas aos Crimes Sexuais no Enfrentamento à Criminalidade. Disponível em: <http://genjuridico.com.br/2018/11/30/as-inovacoes-legislativas-aos-crimes-sexuais-no-enfrentamento-a-criminalidade/>. Acesso em: 03 jun. 2019.

JÚNIOR, Joaquim Leitão; OLIVEIRA, Marcel Gomes de. COMENTÁRIOS À LEI Nº. 13.772 DE 2018: o novo conceito de violência psicológica da Lei Maria da Penha e o novo delito do art. 216-B do Código Penal Brasileiro. Disponível em: <http://portaljuridicobrasil.com.br/sergiocdreis/coment%C3%A1rios-%C3%A0-lei-n%C2%BA-13772-de-2018-o-novo-conceito-de-viol%C3%AAncia-psicol%C3%B3gica-da-lei>. Acesso em: 15 abr. 2019.

LIMA, Simão Prado. Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 06 mai. 2019.

LINHARES, Luis Carlos Oliveira e outros. A inviolabilidade à privacidade (intimidade, vida privada, honra e imagem): CF/88 x atual realidade. Disponível em: <https://jus.com.br/artigos/60125/a-inviolabilidade-a-privacidade-intimidade-vida-privada-honra-e-imagem-cf-88-x-atual-realidade>. Acesso em: 07 mai. 2019.

SILVA, Camila Requião Fentanes da. Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos. Disponível em: <https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos>. Acesso em: 22 abr. 2019.

SOUSA, Matheus Herren Falivene de. Comentário ao art. 218-C do Código Penal. Disponível em: <https://matheusfalivene.jusbrasil.com.br/artigos/630364992/comentario-ao-art-218-c-do-codigo-penal>. Acesso em: 03 jun. 2019.

_____. Como países enfrentam a disseminação não consentida de imagens íntimas?. Disponível em: <http://www.internetlab.org.br/pt/desigualdades-e-identidades/mapa-pornografia-de-vinganca/>. Acesso em: 01 mai. 2019.