I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

PENAL, PROCESSO PENAL, CRIMINOLOGIA E NOVAS TECNOLOGIAS

P397
Penal, processo penal, criminologia e novas tecnologias [Recurso eletrônico on-line] organização I Congresso de Tecnologias Aplicadas ao Direito – Belo Horizonte;

Coordenadores: Guilherme Augusto Portugal Braga, Enio Luiz de Carvalho Biaggi e Lícia Jocilene das Neves – Belo Horizonte, 2017.

Inclui bibliografia
ISBN: 978-85-5505-663-5
Modo de acesso: www.conpedi.org.br em publicações
Tema: O problema do acesso à justiça e a tecnologia no século XXI

1. Direito. 2. Tecnologia. 3. Direito Penal. 4. Processo Penal. 5. Criminologia. I. I Congresso de Tecnologias Aplicadas ao Direito (1:2018 : Belo Horizonte, BH).

CDU: 34

I CONGRESSO DE TECNOLOGIAS APLICADAS AO DIREITO

PENAL, PROCESSO PENAL, CRIMINOLOGIA E NOVAS TECNOLOGIAS

Apresentação

É com imensa satisfação que apresentamos os trabalhos científicos incluídos nesta publicação, que foram apresentados durante o I Congresso de Tecnologias Aplicadas ao Direito nos dias 14 e 15 de junho de 2018. As atividades ocorreram nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, e tiveram inspiração no tema geral "O problema do acesso à justiça e a tecnologia no século XXI".

O evento foi uma realização do Programa RECAJ-UFMG – Solução de Conflitos e Acesso à Justiça da Faculdade de Direito da UFMG em parceria com o Direito Integral da Escola Superior Dom Helder Câmara. Foram apoiadores: o Conselho Nacional de Pesquisa e Pós-graduação em Direito - CONPEDI, EMGE – Escola de Engenharia, a Escola Judicial do Tribunal Regional do Trabalho da 3ª Região, a Federação Nacional dos Pós-graduandos em Direito – FEPODI e o Projeto Startup Dom.

A apresentação dos trabalhos abriu caminho para uma importante discussão, em que os pesquisadores do Direito, oriundos de dez Estados diferentes da Federação, puderam interagir em torno de questões teóricas e práticas, levando-se em consideração a temática central do grupo. Foram debatidos os desafios que as linhas de pesquisa enfrentam no tocante ao estudo do Direito e sua relação com a tecnologia nas mais diversas searas jurídicas.

Na coletânea que agora vem a público, encontram-se os resultados de pesquisas desenvolvidas em diversos Programas de Pós-graduação em Direito, nos níveis de Mestrado e Doutorado, e, principalmente, pesquisas oriundas dos programas de iniciação científica, isto é, trabalhos realizados por graduandos em Direito e seus orientadores. Os trabalhos foram rigorosamente selecionados, por meio de dupla avaliação cega por pares no sistema eletrônico desenvolvido pelo CONPEDI. Desta forma, estão inseridos no universo das 350 (trezentas e cinquenta) pesquisas do evento ora publicadas, que guardam sintonia direta com este Grupo de Trabalho.

Agradecemos a todos os pesquisadores pela sua inestimável colaboração e desejamos uma ótima e proveitosa leitura!

CRIMES VIRTUAIS NO CONTEXTO BRASILEIRO

VIRTUAL CRIMES IN THE BRAZILIAN CONTEXT

Eduardo Cristian Ferreira e Oliveira
Ghabriel Figueiredo de Abreu Oliveira

Resumo

Os avanços tecnológicos, a globalização e a facilidade de acesso à internet no século XXI abriram um espaço intenso de troca de informações por segundo. Desse modo, ficou fácil realizar compras, enviar mensagens, expressar-se publicamente e até acessar uma conta bancária. Entretanto, criminosos aproveitam dessa facilidade para atingir as pessoas e cometerem delitos, como difamação – cyberbullying – golpes virtuais e até falsidade ideológica, criando perfis em redes sociais buscando atingir a vida pessoal de uma pessoa (os fakes). Todos esses crimes podem ser enquadrados no Código Penal Brasileiro resultando em punições como pagamento de indenização ou prisão.

Palavras-chave: Crimes virtuais, Redes sociais, Globalização, Código penal brasileiro

Abstract/Resumen/Résumé

Technological advances, globalization and ease of access to the internet in the 21st century up an intense space for information exchange per second. This made it easy to shop, send messages, express yourself publicly and even access a bank account. However, criminals take advantage of this facility to target people and commit crimes, such as defamation – like cyberbullying - and even ideological falsehood, creating profiles on social media seeking to reach a person's personal life (the fakes). All such crimes can be framed in the Brazilian Penal Code resulting in punishment as compensation or imprisonment.

Keywords/Palabras-claves/Mots-clés: Virtual crimes, Social media, Globalization, Brazilian penal code

1. INTRODUÇÃO

O fenômeno da globalização, impulsionado através dos avanços tecnológicos fez com que o acesso dos indivíduos à informação fosse facilitado, desenvolvendo um ambiente de constante troca de informações e dados em velocidade instantânea. A plataforma de troca de dados – internet – ampliou a capacidade do indivíduo de atuação, utilizando-se da conectividade para a realização compras, envio mensagens, expressar-se publicamente e até acessar uma conta bancária.

As novas possibilidades deste ambiente integrado facilitaram também a atuação de criminosos. Cerca de 62,2 milhões de brasileiros foram vítimas de crimes cibernéticos em 2017, os dados são do relatório anual *Norton Cyber Security Insights*. Entre os compradores virtuais no país, o prejuízo causado pelos delitos foi de aproximadamente 71 bilhões de reais.

A carência de regulamentação especifica ao tema e a falta de denúncias por parte dos membros da comunidade virtual, acaba por gerar uma sensação de impunidade, que corrobora para que novos atos criminosos aconteçam.

Independente de uma legislação especifica ao tema, quando o ambiente virtual é utilizado para a prática de delitos e violência, eles serão adaptados ao código penal brasileiro já existente e os agressores e golpistas serão punidos da mesma forma.

O presente estudo tem por fim estabelecer o referencial teórico do que é “Crime Virtual” e apresentar como a legislação atual brasileira é aplicada nesse contexto.

O presente trabalho se justifica ante o crescente número de crimes virtuais praticado no Brasil e tem por finalidade estabelecer o referencial teórico do que é “Crime Virtual”, apresentando como a legislação atual brasileira é aplicada nesse contexto. O método de pesquisa utilizado foi a revisão bibliográfica.

É de responsabilidade da comunidade virtual a denúncia da ocorrência de crimes, para que novos delitos não ocorram.

2. CONCEITO DE CRIME VIRTUAL E SUAS CLASSIFICAÇÕES

Para se entender o conceito de crimes virtuais, é necessário entender a diferença entre a definição de Hacker e Cracker, além das suas áreas de atuação.

A palavra Hacker, traduzida para o português significa “cortador”, ou seja, o indivíduo corta, invade barreiras virtuais. A função do hacker não é causar mal, ele utiliza a sua alta noção e capacidade de invadir sistemas para colaborar coma justiça, como investigações.

Já o Cracker é uma pessoa que possui o mesmo conhecimento e habilidades de informática, mas, por meios ilícitos, comete delitos fraudando sistemas, invadindo contas alheias e roubando informações sigilosas.

Ou seja, o hacker constrói coisas, e o cracker, quebra elas.

Para Nicholas Ferreira, um exemplo de atitude de um hacker é:

> [...] O hacker encontra uma falha de segurança no site da polícia federal, e com a exploração dessa falha ele teria acesso ao sistema de busca de indivíduos por CPF, uma espécie de consulta. Então ele entra em contato com o webmaster do site avisando da falha, sem causar nenhum dano e sem divulgar nada publicamente sobre a falha. (FERREIRA, 2014, p.5)

E uma atitude de um cracker é:

> [...] O cracker encontra uma falha em um dos servidores do Outlook, que permite que ele envie email para qualquer pessoa se passando por outra. Ao invés de alertar à Microsoft sobre a falha, ele a explora e consegue usá-la a seu favor, para enviar spam para várias pessoas. (FERREIRA, 2014, p.5)

Visto que a internet tem um vasto de acervo de informações preciosas e guarda riquezas no ambiente virtual, criminosos do mundo todo passaram a utilizar o meio informático para cometer delitos.

Especialistas no assunto explicam o que é o crime cibernético.

De acordo com Augusto Rossini – procurador de justiça criminal:

> [...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança 22 informática, que tem por elementos a integridade, a disponibilidade a confidencialidade. (ROSSINI, 2004, p. 110).

O procurador classifica os crimes cibernéticos não só aqueles cometidos via internet, mas sim toda conduta que se envolva com os sistemas da informática.

A classificação dos crimes virtuais se divide em próprios e impróprios.

Os crimes virtuais próprios são aqueles que o criminoso utiliza obrigatoriamente do computador da vítima, ocorrendo a invasão de dados pessoais e fraude de informações para atingir o dispositivo, seja no hardware ou no software.

Para o doutrinador Marco Tulio Viana, os crimes virtuais próprios “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).” (VIANA, 2003, p. 13-26)

Já os crimes virtuais impróprios são aqueles em que é utilizado um computador para a ação ilícita, que já está sob tutela. São crimes que já existem, e são delitos que usufruem, agora, da técnica da informática e seus componentes, como a pedofilia, o estelionato, calúnia, bullying, entre outros.

Quanto aos protagonistas do crime (quem pratica e quem sofre) ficam classificados como sujeitos ativos e passivos.

Os sujeitos ativos são aqueles que cometem o crime, diretamente (como a disseminação de pornografia infantil). A acusação do autor do crime é muito difícil devido a sua ausência física e ao fácil anonimato da internet. Desse modo, foi necessária a criação de grupos especialistas em crimes virtuais e investigações, citados no começo do tópico 2, os Hackers, especializados em investigação virtual e na colaboração com a justiça.

Por conseguinte, os sujeitos passivos são as vítimas, ou seja, quem sofre os prejuízos causados pelo sujeito ativo (autor do crime). Essas vítimas podem ser tanto uma pessoa física, ou até uma pessoa jurídica (como uma empresa), tendo, por exemplo, suas informações fraudadas.

Entretanto, muitos crimes praticados não são divulgados, muitas vezes pela falta de denúncias (por exemplo: empresas não se submetem a divulgação para não aparentarem frágeis ou uma crise).

3. LEGISLAÇÃO NACIONAL EM RELAÇÃO AOS CRIMES VIRTUAIS

Essa nova modalidade criminal é de difícil tipificação, tratando a internet não como um meio e sim como um novo tipo penal, e levando em consideração, também, que há crimes que surgiram juntamente com a internet e o computador. Dessa forma, a legislação nacional teve de se adaptar a essa nova modalidade criminal.

3.1. A LEI CAROLINA DIECKMANN – INVASÃO DE PRIVACIDADE

A lei 12.737/2012 surgiu posteriormente ao evento de invasão de privacidade ocorrido com a atriz brasileira Carolina Dieckmann. Em maio de 2012, a atriz teve 36 fotos e conversas em situações íntimas copiadas por Crackers e divulgadas em mídia pública, após

receber chantagem e pedidos de dinheiro por parte dos invasores para que não divulgassem sua intimidade.

Esta lei teve como objetivo tipificar e acrescentar ao código penal punições para crimes cometidos no ambiente virtual.

A nova lei acresceu os Artigos 154-A e o 154-B ao Código Penal, além de alterar o Artigo 266 e o Artigo 298.

No Artigo 154-A, fica declarado que:

> 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 [...] (BRASIL, 2012).

E no Artigo 154-B, menciona-se:

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

Dessa forma, a lei foi sancionada para evitar e punir novos ataques cibernéticos e não deixar a internet como uma “terra sem lei”. Além disso, por analogia, tornou condutas ilícitas virtuais criminosas como as condutas reais, como no Art. 266:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. Parágrafo único - Aplicam-se as penas em dobro, se o crime é cometido por ocasião de calamidade pública. [...] (BRASIL,2012).

E o Art. 298:

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

Esse artigo da Lei Carolina Dieckmann determina que os cartões de crédito e débito passem a ser documentos pessoais, alcançando o mesmo valor do RG e do CPF e designando sua falsificação como um crime de falsificação de documento particular.

3.2. LEGISLAÇÃO POR FORA DA LEI 12.737/2012

Entretanto, mesmo com a lei 12.737/2012 existe uma carência de um conjunto de sanções jurídicas dedicadas especificamente aos crimes virtuais. Porém, mesmo não existindo essa legislação, quando o meio cibernético é usado para a prática de delito, os crimes são adaptados ao código penal já existente e os criminosos são punidos igualmente.

Algumas dessas condutas criminosas são:

a) Crimes contra a honra (arts. 138,139 e 140 do CP);
b) Crime de ameaça (art. 147 do CP);
c) Furto (art. 155 do CP);
d) Extorsão (art. 158 do CP);
e) Extorsão Indireta (art. 160 do CP);
f) Apropriação indébita (art. 168 do CP);
g) Estelionato (art. 171 do CP);
h) Violação de direito autoral (art. 184 do CP);
i) Escárnio por motivo de religião (art. 208 do CP);
j) Favorecimento da prostituição (art. 228 do CP);
k) Ato obsceno (art.233 do CP);
l) Escrito ou objeto obsceno (art. 234 do CP);
m) Incitação ao crime (art. 286 do CP);
n) Apologia de crime ou criminoso (art. 287 do CP);
o) Pedofilia (art. 241 da Lei 8.069/90);
p) Crime de divulgação do nazismo (art. 20º §2º. da Lei 7.716/89).

4. CONCLUSÃO

A análise sobre os "Crimes Virtuais" nos aponta que a legislação brasileira vigente apesar de não ser especifica quanto ao território digital é suficiente forte para impor sanções jurídicas aos infratores, e com a denúncia dos crimes pela comunidade digital novos delitos tendem a não ocorrer.

REFERÊNCIAS

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Extraído de: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 19 abr. 2018.

CASSANTI, Moisés de Oliveira. **O que são crimes virtuais?**. 2016. Disponível em: <http://idciber.eb.mil.br/index.php?option=com_content&view=article&id=795:o-que-sao-crimes-virtuais&catid=78&Itemid=301>. Acesso em: 19 abr. 2018.

FERREIRA, Nicholas. **O Guia do Hacker.** 2014. Disponível em: <http://www.guiadohacker.com.br/O_Guia_do_Hacker_1_edicao.pdf>. Acesso em: 19 abr. 2018.

ROSSINI, Augusto Eduardo de Souza**. Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica, 2004.

SANTO, Kleber Assunção do Espírito. **Crimes Cibernéticos**. 2015. 49 f. TCC (Graduação) - Curso de Direito, Universidade Tuiuti do Paraná, Curitiba, 2015. Disponível em: <http://tcconline.utp.br/media/tcc/2015/09/CRIMES-CIBERNETICOS.pdf>. Acesso em: 19 abr. 2018.

VIANA, Marco Túlio. **Fundamentos de direito penal informático**. Do acesso não autorizado a sistemas computacionais. Rio de Janeiro: Forense, 2003, p. 13-26.