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!

CIBERCRIME: CIBERTERRORISMO E O PROCESSO PENAL

CYBERCRIME: CYBERTERRORISM AND THE CRIMINAL PROCEDURE

Andressa Laryssa Leocadio Januário
Ricardo Vitor da Silva

Resumo

A pesquisa objetiva explicar e esclarecer um dos problemas atuais da era da informação, o ciberterrorismo. O ciberespaço é um ambiente que surgiu com o desenvolvimento e aprimoramento da tecnologia de informação e comunicação, ele é um espaço constituído por um conjunto de redes que contém variados tipos de conhecimentos. Pelo fato do ciberespaço ser uma área de grande poder informativo é notável a presença de grupos os quais praticam variados crimes no espaço virtual, visto que ele é palco para o terrorismo cibernético, o qual é uma problemática bem comum na contemporaneidade.

Palavras-chave: Ciberterrorismo, Penal, Tecnologia, Cibercrime, Terrorismo

Abstract/Resumen/Résumé

The research aims to explain and clarify one of the current problems of the information age, the cyberterrorism. Cyberspace is an ambience that has emerged with the development and improvement of information and communication technology, it is a space made up of a set of networks that contain different types of knowledge. Because cyberspace is an area of great information power, seeing that it is notable the presence of groups that practice various crimes in virtual space, it is the stage for cyber terrorism, which is a problematic very common in contemporary times.

Keywords/Palabras-claves/Mots-clés: Cyberterrorism, Criminal, Technology, Cybercrime, Terrorism

CIBERCRIME: CIBERTERRORISMO E O PROCESSO PENAL

CYBERCRIME: CYBERTERRORISM AND THE CRIMINAL PROCEDURE

Andressa Laryssa Leocadio Januário

Ricardo Vitor da Silva

Resumo

A pesquisa objetiva explicar e esclarecer um dos problemas atuais da era da informação, o ciberterrorismo. O ciberespaço é um ambiente que surgiu com o desenvolvimento e aprimoramento da tecnologia de informação e comunicação, ele é um espaço constituído por um conjunto de redes que contém variados tipos de conhecimentos. Pelo fato do ciberespaço ser uma área de grande poder informativo é notável a presença de grupos os quais praticam variados crimes no espaço virtual, visto que ele é palco para o terrorismo cibernético, o qual é uma problemática bem comum na contemporaneidade.

Palavras-chave: Ciberterrorismo, Penal, Tecnologia; Cibercrime, Terrorismo.

Abstract

The research aims to explain and clarify one of the current problems of the information age, the cyberterrorism. Cyberspace is an ambience that has emerged with the development and improvement of information and communication technology, it is a space made up of a set of networks that contain different types of knowledge. Because cyberspace is an area of great information power, seeing that it is notable the presence of groups that practice various crimes in virtual space, it is the stage for cyber terrorism, which is a problematic very common in contemporary times.

Keywords: Cyberterrorism, Criminal, Technology, Cybercrime, Terrorism.

INTRODUÇÃO

A Terceira Revolução Industrial iniciou se depois da Segunda Guerra Mundial e durante a Guerra Fria. Nessa nova era houve o desenvolvimento de novas tecnologias a partir da conexão entre as ciências e as produções das indústrias e, consequentemente, houve o facilitamento da reprodução de informações pelo mundo e o desenvolvimento de novas

inteligências. Na década de 1960, durante a Guerra Fria, a busca pelo controle mundial e a preeminência política trouxe a necessidade do surgimento da rede, que colaborou na troca e conservação de informes sigilosos.

> O governo norte-americano queria desenvolver um sistema para que seus computadores militares pudessem trocar informações entre si, de uma base militar para a outra e que mesmo em caso de ataque nuclear os dados fossem preservados. Seria uma tecnologia de resistência. Foi assim que surgiu então a ARPANET, o antecessor da internet, um projeto iniciado pelo Departamento de Defesa dos Estados Unidos que realizou então a interconexão de computadores, através de um sistema conhecido como comutação de pacotes, que é um esquema de transmissão de dados em rede de computadores no qual as informações são divididas em pequenos "pacotes", que por sua vez contém trecho de dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original. (HISTÓRIA, 2010, p. 2).

A rede estabeleceu-se, finalmente, na década de 1970 e marcou o inicio da internet. Segundo Castells (2003), a Internet é um meio de comunicação que possibilita a interlocução entre muitos e em alcance mundial.

> "No final do século XX, três processos independentes se uniram, inaugurando uma nova estrutura social predominantemente baseada em redes: as exigências da economia por flexibilidade administrativa e por globalização do capital, da produção e do comércio; as demandas da sociedade, em que os valores da liberdade individual e da comunicação aberta tornaram-se supremos; e os avanços extraordinários na computação e nas telecomunicações possibilitados pela revolução microeletrônica. Sob essas condições, a Internet, uma tecnologia obscura sem muita aplicação além dos mundos isolados dos cientistas computacionais, dos hackers e das comunidades contra culturais, tornou-se a alavanca na transição para uma nova forma de sociedade — a sociedade de rede —, e com ela para uma nova economia." (CASTELLS, 2003, p.8).

O expressivo crescimento do ciberespaço acarretou na grande dependência da população mundial pela rede de Internet. Um número considerável de pessoas resolvem suas questões financeiras, questões empresariais e pessoais no meio virtual, em vista disso a segurança nesse meio é fundamental para manter as informações em privado. O grande número de pessoas utilizando a Internet para variados fins possibilitou o crescimento notável de indivíduos que cometem crimes no ciberespaço. Estes podem operar de diversos lugares e ultrapassar fronteiras da jurisdição em todo o mundo, e esse amplo território online permitiu o crescimento do índice de crimes virtuais, incluindo o terrorismo cibernético.

O CIBERTERRORISMO

Com a disseminação da internet e o crescimento da guerra de informações nos anos 90, houve uma grande discussão no país desenvolvedor da Internet, os EUA, em relação à

possibilidade do terrorismo também se inserir no meio virtual e usar a internet como arma contra o governo americano.

De acordo com o Conselho Nacional de Pesquisa (1991), um conselho dos Estados Unidos responsável por produzir relatórios e proporcionar a busca por ciência, “O terrorista de amanhã pode ser capaz de causar mais danos com um teclado do que com uma bomba.”. Em consequência disso o ciberterrorismo foi colocado como uma ameaça à segurança do Estado. O ciberterrorismo é considerado um dos crimes mais perigosos da Internet, além de comprometer o funcionamento de sites governamentais, afeta também o funcionamento de aparelhos tecnológicos e das bases de uma organização federal.

> Um ato criminoso perpetrado pelo uso de computadores e telecomunicações deficiências, resultando em violência, destruição e / ou interrupção de serviços, onde o objetivo pretendido é criar medo, causando confusão e incerteza dentro uma determinada população, com o objetivo de influenciar um governo ou população a conformar-se a uma agenda política, social ou ideológica específica (FBI, 2004).

Há uma grande diferença entre hacker e ciberterrorista, mesmo que ambos tenham um grande conhecimento técnico em relação à ciência da computação e da rede. O hacker usa de seus conhecimentos para usufruto próprio e não tem uma motivação exata, podem invadir computadores pela simples curiosidade, para fins profissionais ou até mesmo crimes. O ciberterrorista tem finalidades puramente políticas, por isso ataca organizações federais com o objetivo de provocar desordem nos sistemas do Estado.

O ataque ciberterrorista mais famoso ocorreu na Estônia em 27 de abril 2007, em que vários sites governamentais ficaram fora do ar, comprometendo assim o sistema do país, visto que a Estônia e totalmente ligada na rede de informações. Os EUA também já sofreram ataques de terroristas cibernéticos, os terroristas eram integrantes da máfia russa e por meio de computadores conseguiram comprometer caixas eletrônicos e maquinas de cassinos.

Segundo o diretor do FBI Robert Muller, agência norte americana de investigação, com a evolução da tecnologia e a facilidade do acesso a Internet os taques de ciberterrorista se igualarão ou ficarão piores do que os ataques de terrorismo não cibernético.

> É muito pouco o que fazemos hoje em dia com os assuntos relacionados com a internet. O roubo de propriedade intelectual, o roubo de investigação e desenvolvimento, o roubo de planos e programas empresariais para o futuro... todos esses assuntos são vulneráveis a serem explorados por atacantes.(MULLER, 2012)

A SITUAÇÃO NO BRASIL

Por volta da década de 1990 um novo meio de comunicação se popularizou aos olhos do mundo, a rede mundial de computadores interligados, caracterizada por um ambiente hostil e sem limites necessitava de legislação para proteger o internauta. Durante um grande período de tempo não havia restrições e nem controles, logo todos poderiam ser qualquer um ou qualquer coisa, e assim a grande dificuldade de governar esse grande ambiente de comunicação sem fronteiras se perdurou por muito tempo. No Brasil as notícias no que se refere a crimes virtuais ganharam força na imprensa somente em 1997. Mas foi somente em 2001 que o país ficou reconhecido mundialmente ao atingir o topo mundial em crimes na internet.

No decorrer deste período uma grande parcela da população aderiu às novas possibilidades ainda não limitadas, os hackers brasileiros aumentavam exponencialmente, o que marcou o período com um grande percentual de Cibercrime como: alteração de conteúdos de "homepages", o roubo de identidades, fraudes de cartão de crédito, invasões a sites e até mesmo violações à propriedade intelectual. Mais tarde no ano de 2005 uma grande operação proposta pela policia federal brasileira, na qual recebeu o nome de operação Pégaso, prendeu 85 pessoas ao expedir 104 mandatos para cerca de sete estados sob a acusação de furto qualificado, formação de quadrilha e violação do sigilo bancário.

A internet evolui cada vez mais rápido do que a capacidade do Estado de legislar, e a necessidade de uma norma para a prevenção de crimes dentro desse meio de comunicação era um fato, mas, somente em 30 de novembro de 2012 entrou em vigência a LEI Nº 12737, que ficou conhecida como lei Carolina Dieckmann.

> Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático"
> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

A atriz que ao se tornar vítima de hackers tem suas informações e fotos pessoais expostas na internet, recorre à justiça o que deu base para a lei Nº 12737/2012 que tipifica os crimes cibernéticos. Mas até hoje grande parte da população no Brasil e no mundo sofre na mão de hackers, usuários que se veem em uma falsa impressão de anonimato e não se limitam às medidas estabelecidos por lei expondo, dessa forma, a carência de assegurar o direito dos

internautas em relação a segurança de informações e garantia da privacidade individual. O Brasil não tem medidas legais relacionadas ao terrorismo cibernético, o Estado necessita de leis que protejam a segurança e a contra inteligência, baseadas em estudo mais profundos e minuciosos sobre os terroristas. O desenvolvimento de estratégia é primordial para a prevenção de ataques e uma melhor medida de segurança e conservação da segurança nacional.

CONCLUSÃO

A Internet é um grande meio de comunicação e, com sua evolução, muitos indivíduos têm acesso. O crescimento do ciberespaço proporcionou o aumento consideráveis de crimes cibernéticos, como o ciberterrorismo. O terrorismo cibernético põe em risco a integridade e a organização do Estado e é de suma importância a ação governamental e legal para a garantia da segurança do país, impedindo ou prevenido ataques terroristas vindos da Internet.

REFERÊNCIAS

BRASIL. **Lei nº 12.737, 30 de novembro de 2012.** Brasília: Planalto, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm >. Acesso em: 11 mar. 2018.

CASTELLS, Manuel. **A Galáxia da Internet.** Trad. Maria Luiza X. de A. Borges. 1. ed. Rio de Janeiro: Zahar, 2003. cap. 1. p. 13.

GARDINI, Mayara Gabrielli. Terrorismo no Ciberespaço: O poder cibernético como ferramenta de atuação de organizações terroristas. **Fronteira:** Revista de iniciação científica em relações internacionais. Belo Horizonte. v.13, n.25 e 26, 2014. Disponível em: <http://periodicos.pucminas.br/index.php/fronteira/article/view/10461.>. Acesso em: 16 mar. 2018.

HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 13/04/2018.

MASANA, Sebastian. **Ciberterrorismo.** 12 mar. 2018 Disponível em: <http://www.informaticaforense.com.co/ciberterrorismo/>. Acesso em: 12 mar. 2018.

NUNES, Paulo Fernandes Viegas. Ciberterrorismo: Aspectos de segurança. **Revista Militar**. n.2433, out. 2004. Disponível em: <https://www.revistamilitar.pt/artigo/428>. Acesso em: 13 mar. 2018.

VELANDIA, Karenina. Quais são as sofisticadas armas cibernéticas da guerra do século 21?. **BBC Mundo.** 5 mar. 2017. Disponível em: < http://www.bbc.com/portuguese/internacional-39149203>. Acesso em: 16 mar. 2018.

WEISER, Benjamin Russian Gang Hacked Slot Machines and Plotted Over Stolen Sweets, U.S. Says. **The New York Times** Disponível em:<https://www.nytimes.com/2017/06/07/nyregion/russian-eurasian-organized-crime.html>. Acesso em: 13 abr. 2018.