SEMINÁRIO NACIONAL DE FORMAÇÃO DE PESQUISADORES E INICIAÇÃO CIENTÍFICA EM DIREITO DA FEPODI

S472
Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito da FEPODI [Recurso eletrônico on-line] organização Federação Nacional dos Pós-Graduandos em Direito - FEPODI;

Coordenadores: Beatriz Souza Costa, Lívia Gaigher Bosio Campello, Yuri Nathan da Costa Lannes – Belo Horizonte: ESDH, 2017.

Inclui bibliografia
ISBN: 978-85-5505-383-2
Modo de acesso: www.conpedi.org.br em publicações

1. Direito – Estudo e ensino (Graduação e Pós-graduação) – Brasil – Congressos nacionais. 2. Direito Constitucional. 3. Direito ambiental. 4. Direito Administrativo. 5. Direito Civil. 6. Direito Penal. 7. Direitos Humanos. 8. Direito Tributário. 9. Filosofia Jurídica. 10. Gênero. 11. Diversidade Sexual. I. Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito da FEPODI (1:2016 : Belo Horizonte, MG).

CDU: 34

FEPODI
FEDERAÇÃO NACIONAL DOS PÓS-GRADUANDOS EM DIREITO

SEMINÁRIO NACIONAL DE FORMAÇÃO DE PESQUISADORES E INICIAÇÃO CIENTÍFICA EM DIREITO DA FEPODI

Apresentação

É com imensa satisfação que a Escola Superior Dom Helder Câmara e a Federação Nacional dos Pós-graduandos em Direito – FEPODI apresentam à comunidade científica os Anais do Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito. Tal produção resulta do exitoso evento sediado nas dependências da Escola Superior Dom Helder Câmara, em Belo Horizonte-MG, nos dias 10 e 11 de outubro de 2016, que contou com o valioso apoio do Conselho Nacional de Pesquisa e Pós-Graduação em Direito – CONPEDI e da Associação Brasileira de Ensino do Direito – ABEDi.

Trata-se de obra coletiva composta por 263 (duzentos e sessenta e três) resumos expandidos apresentados no seminário e que atingiram nota mínima de aprovação dentre os 318 (trezentos e dezoito) trabalhos submetidos ao evento. As comunicações científicas estão organizadas em 21 (vinte e um) Grupos de Trabalho ligados a diversas áreas do direito, inseridos num ambiente de ricos debates e profundas trocas de experiências entre os representantes das mais diversas localidades do Brasil.

Os referidos Grupos de Trabalho contaram, ainda, com a contribuição de proeminentes docentes ligados a renomadas instituições de ensino superior do país, os quais indicaram os caminhos para o aperfeiçoamento dos trabalhos dos autores, afim de que eles estejam aptos, após desenvolvimento, a serem publicados posteriormente nos periódicos jurídicos nacionais.

Neste prisma, os presentes anais, de inegável valor científico, já demonstram uma contribuição para a pesquisa no Direito e asseguram o cumprimento dos objetivos principais do evento de fomentar o aprofundamento da relação entre pós-graduação e graduação em Direito no Brasil, bem como de desenvolver os pesquisadores em Direito participantes do evento por meio de atividades de formação em metodologias científicas aplicadas.

Uma boa leitura a todos!

Beatriz Souza Costa

Lívia Gaigher Bosio Campello

Yuri Nathan da Costa Lannes

Coordenadores Gerais do Seminário Nacional de Formação de Pesquisadores e Iniciação Científica em Direito.

A REGULAMENTAÇÃO JURÍDICA DA DEEP WEB: DESAFIOS CONTEMPORÂNEOS DO COMBATE AOS CRIMES VIRTUAIS.

LA REGULAMENTACIÓN JURÍDICA DE LA DEEP WEB: DESAFIOS ATUALES DEL COMBATE A LOS CRINEMES VIRTUALES.

Nathália Miranda da Silva
Anderson Alves de Morais
Caio Augusto Souza Lara

Resumo

A pesquisa moderna faz menção à regulamentação da Deep Web, evidenciando as dificuldades da criação de uma legislação internacional e da identificação do criminoso. Demonstra-se que a Deep Web, por garantir o anonimato, abre espaço para vários crimes. O crescente aumento desses crimes, revelado por pesquisas recentes, aponta para a necessidade urgente de cooperação entre os países para a solução do problema. A pesquisa demonstra que as políticas estabelecidas nos países até o momento e a criação de um tratado internacional, não foram suficientes para combater os crimes. O desafio consiste em criar medidas eficazes para combater o cibercrime.

Palavras-chave: Crime virtual, Direito internacional, Direitos humanos, Regulamentação jurídica, Deep web, Direito cibernético

Abstract/Resumen/Résumé

La investigación moderna hace mención a la regulación de la Deep Web, poniendo en evidencia las dificultades de la creación de una legislación internacional y de la identificación del criminal. Se muestra que la Deep Web, por garantizar el anonimato, abre espacio para diversos delitos. La investigación muestra que las políticas establecidas em los países hasta el presente momento y la creación de un acuerdo internacional, no se hicieron suficientes para el combate de los crímenes. El desafio está en crear medidas efictivas para el combate del cibercrimene.

Keywords/Palabras-claves/Mots-clés: Crímene virtual, Derecho internacional, Derechos humanos, Regulamentación jurídica, Deep web, Derecho cibernético

1 CONSIDERAÇÕES INICIAIS

A presente pesquisa trata da questão da regulamentação jurídica da Deep Web tendo em vista os desafios atuais de combate aos crimes praticados por meio dessa. Esses desafios se pautam, principalmente, na complexidade de formulação de uma legislação internacional e de identificação do cibercriminoso.

Apesar de existir há muito tempo, a internet obscura tem ganhado, atualmente, maior repercussão internacional. O aumento de sua utilização, atrelado ao crescimento significativo do acesso da população mundial à internet, facilitou a prática de crimes como pedofilia, prostituição, tráfico de armas, de drogas, de órgãos, roubo de dados e ação de hackers que conseguem invadir, por exemplo, programas sigilosos de empresas e órgãos públicos.

Em relação à regulamentação, vários países adotaram uma legislação interna para regulamentar a Deep Web, além de criarem um tratado internacional conhecido como Convenção de Budapeste para tratar sobre o cibercrime. Entretanto, o combate é ineficaz, visto que a regulamentação atual que diz respeito às formas de punir os crimes, não atinge seu objetivo devido ao fato do cibercriminoso conseguir facilmente transpor as fronteiras de seu país e o seu reconhecimento ser impossibilitado devido ao anonimato garantido pela Deep Web.

A pesquisa que se propõe pertence à vertente metodológica jurídico-sociológica. No tocante ao tipo de investigação, foi escolhido, na classificação de Witker (1985) e Gustin (2010), foi o tipo jurídico-projetivo e a técnica de pesquisa, a pesquisa teórica. Dessa forma, a pesquisa se propõe analisar os mecanismos jurídicos internacionais de combate aos crimes praticados por meio da Deep Web.

2 DEEP WEB

A Deep Web, também conhecida como Dark Web, consiste em uma área da internet que possui conteúdos não encontrados na web convencional e são dificilmente rastreáveis ou monitorados por sites de busca, além de ter como característica fundamental, o anonimato de

seus usuários, garantido por um sistema de criptografias. A internet que conhecemos e que temos acesso, onde fazemos nossas pesquisas, chamada de Surface Web, corresponde a apenas 10% de todo o conteúdo existente no mundo virtual, enquanto a *Deep Web* abarcaria os outros 90%. Ao se fazer uma analogia com um iceberg, seria como se a Surface Web fosse a ponta do iceberg, aquilo que fica na superfície, enquanto a *Deep Web* seria a imensidão de massa de gelo abaixo da superfície, algo que não temos dimensão do tamanho e conteúdo.

> [...] informações públicas na Deep Web são comumente de 400 a 500 vezes maiorer que as definidas da World Wide Web. A Deep Web contém 7.500 terabytes de informações comparadas a 19 terabytes de informação da Surface Web. A Deep Web contém aproximadamente 550 bilhões de documentos individuais comparados com 1 bilhão da Surface Web. Existem mais de duzentos mil sites atualmente na Deep Web. Seis das maiores enciclopédias da Deep Web contém cerca de 750 terabytes de informação, suficiente para exceder o tamanho da Surface Web quatro vezes. Em média, os sites da Deep Web recebem 50% mais tráfego mensal, ainda que não sejam conhecidos pelo público em geral. A Deep Web é a categoria que mais cresce no número de novas informações sobre a Internet. Deep Web tende a ser mais estrita, com conteúdo mais profundo, do que sites convencionais. A profundidade de conteúdo de qualidade total da Deep Web é de 1.000 a 2.000 mil vezes maior que a da superfície. O conteúdo da Deep Web é altamente relevante para todas as necessidades de informação, mercado e domínio. Mais da metade do conteúdo da Deep Web reside em tópicos específicos em bancos de dados. Um total 95% da Deep Web é informação acessível ao público não sujeita a taxas ou assinaturas [...] (POMPÉO; SEEFELDT, 2013)

A Deep Web é dividida em camadas, quanto mais profunda é a camada, mais obscuro é o seu conteúdo e mais difícil é de acessá-la. O acesso inicial geralmente se dá por uma ferramenta chamada TOR (The Onion Routher), uma plataforma criada pela marinha norte-americana que visava prover a segurança e privacidade. Após o abandono do projeto pelos militares, passou a ser desenvolvida por algumas organizações virtuais, sendo seu propósito, a partir de um sistema sigiloso, garantir o anonimato e segurança dos usuários. O acesso às demais camadas exige uma combinação de letras criptografadas, e muitas vezes de acesso restrito, como se fossem senhas de alta segurança, ou seja, a navegação feita por elas é distribuída por diversos caminhos, não permitindo o rastreio direto à fonte das informações que estão sendo trocadas.

Dessa forma, a navegação pela Deep Web fornece muito mais segurança àqueles que não querem ser identificados do que a navegação pela web comum, sendo, portanto, dificilmente controlada pelo Governo e polícia. A garantia da comunicação entre os

internautas sem o risco de identificação ou interceptações abriu espaço para o aparecimento de cibercriminosos, que, apropriando-se do incógnito, começaram a praticar diversos atos ilícitos. Pode-se somar aos fatores que influenciaram a utilização da Deep Web como um meio ideal para a prática de vários crimes, a inexistência de uma regulamentação eficaz, motivo pelo qual a Dark Web é conhecida como uma terra sem lei.

> [...] Partindo de uma análise perfunctória da relação estabelecida entre o meio eletrônico com o homem, é possível a previsibilidade de chances maiores no cometimento de delitos no *cyber* espaço, tendo em vista que o usuário de tal meio se sente inatingível pela punição decorrente de um delito praticado por meio eletrônico, face à insegurança jurídica e a falta de preparação por parte do Estado, em dar continuidade às investigações, ou até mesmo de como proceder à investigação de delitos desta classe. Percebe-se de forma indutiva que muitos indivíduos que não seriam capazes de cometer delitos nas relações concretas (indivíduo x indivíduo), encontram no meio virtual segurança para o cometimento de delitos, seja tendo o virtual como meio (tráfico de drogas), seja como forma direta de prática de crime (estelionato) [...]. (SILVA, 2015)

Algumas das práticas ilegais mais recorrentes são o tráfico de órgãos, de dados, de pessoas, de drogas, sendo o mais famoso o Silk Road, descoberto pelo FBI em 2013. Há ainda a prostituição e pornografia infantil, as encomendas de assassinos de aluguel, as conexões terroristas, comércio das chamadas bonecas sexuais humanas, sendo esse último um dos mais abomináveis e cruéis crimes e que apenas uma pequena parcela da população tem conhecimento. As bonecas sexuais são meninas, geralmente entre 8 e 12 anos e de origem pobre, que são compradas pelos "Doll Makers", por um ínfimo preço, e passam por procedimentos cirúrgicos, onde são retirados seus braços, pernas, cordas vocais e dentes e são substituídos por próteses, com o objetivo de não oferecer nenhuma resistência às perversões do dono. Elas são encomendadas e vendidas por um preço exorbitante e tem uma estimativa de vida de um ano após a cirurgia.

Os crimes que lá ocorrem são ainda facilitados pelo uso dos *bitcoins*, moedas virtuais criptografadas, que movimentam dinheiro de verdade e permitem transações anônimas. A rede *bitcoin* funciona de forma autônoma, sem um banco de dados central ou único administrador central, dessa forma os usuários podem transacionar diretamente uns com os outros sem a necessidade de um intermediário. O fato de não haver uma autoridade ou base de dados central, pois se trata de uma rede descentralizada, faz com que seja um grande desafio aos agentes da lei detectar atividades suspeitas, identificar usuários, obter registros das

transações e, consequentemente, iniciar uma ação penal, logo o cibercriminoso se utiliza dessa incerteza legal para praticar inúmeros crimes.

3 A REGULAMENTAÇÃO JURÍDICA DA DEEP WEB

Diante da gravidade dos crimes que estão sendo cometidos na Deep Web e do seu aumento nos últimos anos, medidas foram tomadas com o intuito de regulamentar o espaço. Vários países como o Japão, Estados Unidos, Itália, Portugal, Brasil e França adequaram sua legislação interna, adotando leis que dizem respeito à punição dos infratores. Como exemplo, Portugal, em 2009, aprovou a Lei do Cibercrime, transpondo para a ordem jurídica interna a decisão relativa à ataques contra sistemas de informação e adaptou o direito interno à Convenção sobre Cibercrime do Conselho da Europa. Também o Brasil, em 2012, aprovou a Lei Carolina Dieckmann que dispõe sobre a tipificação criminal dos delitos informáticos, e em 2014 aprovou o Marco Civil da Internet, lei que disciplina o uso da internet no Brasil tendo como fundamento o respeito à liberdade de expressão, além de estabelecer princípios, garantias, direitos e deveres para o seu uso.

Tendo em vista a possibilidade dos utilizadores transporem seus territórios, o que configura crime em escala global, criou-se, também, um tratado internacional, assinado por 11 países, conhecido como Convenção de Budapeste. Essa consiste na harmonização das legislações penais e processuais sobre crime virtual e, é hoje, o único instrumento jurídico de caráter global para combater o cibercrime. Porém, tanto o tratado internacional, quanto as regulamentações internas de cada país tem se mostrado ineficientes no combate aos crimes praticados por meio da Deep Web, uma vez que o número de atos ilícitos, segundo estatísticas e pesquisas, não só persiste, como aumenta.

> Norteando-se pela atual situação do Brasil e de outros países na complexa tarefa de combate aos cibercrimes, é possível verificar como alternativa, com grandes chances de êxito em sua eficácia, a assinatura do Brasil à Convenção de Budapeste, já assinada por vários países da Europa, que trata o cibercrime desde a sua definição até normas procedimentais, aliada à cooperação penal internacional, tanto na sua investigação quanto na sua produção probatória, devendo esta ser oficialmente assinada uma vez que somente se confere de forma concreta a cooperação internacional através de documento oficialmente assinado pelos países participantes. Convém ainda destacar, que a convenção não obsta aos Estados signatários a criação das medidas legislativas que acharem necessárias para a prevenção e repressão dos cibercrimes, demonstrando ainda, que ao aderir à convenção é possível criar uma "relação de circulação" entre o direito material e processual que

> permeia a era dos crimes eletrônicos, para que a partir de uma legislação específica seja possível buscar procedimentos eficazes e concretos ao tratamento desses delitos (SILVA, 2013).

A ineficiência das varias legislações internas deve-se em parte à facilidade do criminoso transpor as fronteiras do seu país e a dificuldade de localização desses. E quanto à regulamentação internacional, uma das barreiras consiste na divergência de valores, cultura, princípios, como a questão da liberdade de expressão, política interna e externa, interesses econômicos, entre os países, o que inviabiliza a formulação de um consenso e de normas que sejam aceitas por todos.

> Persiste a necessidade de estabelecer normas globais e padrões para reger a conduta e comportamento no mundo virtual. Apesar da necessidade, as políticas nacionais e regionais podem colidir com essa normatização global. Isto exige regulamentação universal ou global considerando o impacto transnacional e arrebatador inerente do cybercrime. Apesar da dificuldade intrínseca na harmonização ou unificação de políticas criminais e penais, sendo uma manifestação de poder soberano e autoridade, as participações no ciberespaço têm instigado os Estados a trilharem por uma nova época de cooperação em matéria de direito penal e público território irregular e vacilante.[...]O objetivo principal da Convenção é harmonizar a legislação penal material e procedimentos de investigação internas. Eram duas as principais preocupações dos redatores da Convenção: a primeira era assegurar que as definições fossem flexíveis a ponto de se amoldar aos novos tipos de crimes e seus métodos e a segunda era manter-se sensível aos regimes jurídicos dos Estados-nação. Estas preocupações foram especialmente desafiadoras na área de direitos humanos, porque os estados têm diferentes valores morais e culturais. Por exemplo, os países europeus têm um grau muito mais elevado de proteção da privacidade do que os Estados Unidos. (CHAWKI; WAHABI, 2006).

Além desse ponto, cabe destacar que essas legislações dizem respeito às formas de punir o cibercriminoso após a sua identificação, o que não ocorre de fato, em detrimento do anonimato garantido pelo sistema de criptografia. Dessa forma, as leis tornam-se obsoletas, visto que não são realmente aplicadas na prática e, portanto não passam de teorias. Alguns órgãos como a CIA, o FBI e a polícia federal de vários países atuam na Deep Web tentando localizar esses criminosos, e apesar desse processo de identificação não ser impossível, é muito difícil, pois quando o cibercriminoso percebe que está sendo investigado ele consegue facilmente apagar seus dados e "sumir do mapa".

Uma das grandes polêmicas no debate atual acerca da regulamentação da Deep Web consiste na necessidade de considerar também seu lado positivo, visto que, apesar de ser um instrumento para várias práticas ilegais, ela também atua como um grande arcabouço de

informações, livros e conhecimentos, que são inexistentes na Surface Web (parte da internet convencional). Além disso, ela funciona como um importante instrumento de manifestação em países repressores e ditatoriais, como por exemplo, no caso da primavera árabe, um movimento contrário ao governo vigente no Mundo Árabe, cujo importante meio de comunicações foi a Deep Web. Dessa forma, o banimento do anonimato, além ferir o princípio básico da liberdade de expressão e direito à privacidade, interferiria diretamente nos benefícios proporcionados por ela.

A grande questão contemporânea acerca do tema é, não somente criar uma regulamentação eficiente da Deep Web, mas também, proporcionar aos países a possibilidade de identificar e punir os criminosos virtuais. Faz-se necessário um consenso mundial a respeito da aceitação e aplicação das propostas legais, haja vista que há discordância em relação ao uso da internet nas várias partes do globo, como por exemplo, na China, onde não é permitido aos cidadãos acesso a alguns mecanismos de pesquisa. Assim como, faz-se necessário também o redirecionamento da discussão mundial para a descoberta de formas eficientes de identificar os criminosos que utilizam a Deep Web para cometer crimes graves.

4 CONSIDERAÇÕES FINAIS

Esta pesquisa se propôs, como objetivo geral, investigar e analisar os mecanismos atuais de regulamentação da Deep Web, bem como a sua eficácia diante do combate aos crimes virtuais. Para isso o trabalho teve como base e fundamento o levantamento dos tipos de crimes praticados na Deep Web, o modo como esses crimes ocorrem, desde o sistema de criptografia à utilização do *bitcoin*, além da capacidade de identificação do criminoso por órgãos internacionais.

A elaboração de uma legislação internacional para regulamentação e combate ao cibercrime é necessária e urgente. Entretanto, cabe ressaltar como entraves a grande divergência e dificuldade de atingir um consenso entre os países, além da incapacidade de identificar o criminoso, o que, caso não seja feito, inviabiliza a aplicação da lei. Tal situação acarreta outro problema que consiste na polêmica do direito à privacidade conferida pela Deep Web, além dos benefícios que ela proporciona por garantir o anonimato.

Logo, percebe-se que a solução para o problema é mais difícil do que parece. Porém, diante das inúmeras atrocidades que estão sendo cometidas na Dark Web, pode-se afirmar que o melhor caminho para combatê-las é dando destaque, na discussão internacional, não

somente para a criação de uma legislação eficiente, mas também para o desenvolvimento de tecnologias avançadas que permitam a identificação do criminoso.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Leonardo. **Cybercrimes na deep web: as dificuldades jurídicas de determinação de autoria nos crimes virtuais.** Portal Jus Navigandi: 06/2015. Disponivel em: <https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais/2>. Acesso em: 02/05/2016.

AVILA, Renato Nogueira Perez. **Deep Web: a internet que não está no Google**. 1ª. ed. São Paulo: Ciência Moderna, 2015

BRASIL. Lei Marco Civil da Internet (lei nº 12.965 de 23 de abril de 2014). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 22/04/2016.

CHAWKI, Mohamed; WAHABI, Mohamed. **Identity theft in cyberspace: issues and solutions.** Disponível em: <https://www.researchgate.net/publication/265082208_Identity_Theft_in_Cyberspace_Issues_and_Solutions>. Acesso em: 23/04/2016.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca. (**Re)pensando a pesquisa jurídica: teoria e prática.** 3ª. ed. Belo Horizonte: Del Rey, 2010.

POMPÉO, Wagner Augusto Hundertmarck; SEEFELDT, Joao Pedro. **Nem tudo está no google: Deep web e o perigo da invisibilidade.** Portal da Universidade Federal de Santa Maria: 06/06/2013. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 22/04/2016

ROHR, Atieres. **Deep web: o que é e como funciona**. Portal G1: 04/02/2016. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/deep-web-o-que-e-e-como-funciona-g1-explica.html>. Acesso em: 16/04/2016.

SILVA, Ana Karolina Calado da. **O estudo comparado dos crimes cibernéticos: uma abordagem instrumentalista-constitucional acerca de sua produção probatória em contraponto à jurisprudência contemporânea brasileira.** Portal de e-governo, inclusão digital e sociedade do conhecimento: 06/04/2015. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/o-estudo-comparado-dos-crimes-cibern%C3%A9ticos-uma-abordagem-instrumentalista-constitucional>. Acesso em: 05/05/2016

SOUZA, Marcos. **Visitando o lado negro da internet (Deep web)**. Youtube: 27/06/2013. Disponível em: <https://www.youtube.com/watch?v=-qtdx2zDeD0>. Acesso em: 16/03/2016.

WITKER, Jorge. **Como elaborar uma tesis en derecho: pautas metodológicas y técnicas para el estudiante o investigador del derecho.** Madrid: Civitas, 1985.