DIÁLOGOS E INTERFACES DO DIREITO

REVISTA CIENTÍFICA DO CURSO DE DIREITO
CENTRO UNIVERSITÁRIO FAG

CIBERCRIMINALIDADE: OS DESAFIOS DA INVESTIGAÇÃO NO COMBATE AS ORGANIZAÇÕES CRIMINOSAS NOS SUBMUNDOS DA INTERNET

FERREIRA, Vanessa Sanabria Trindade[1]
FADEL, Alex[2]

RESUMO:

O presente artigo busca analisar os problemas enfrentados com a constante expansão tecnológica, a qual tem facilitado a comunicação mundial, atraindo para o mundo digital toda sociedade que procura sempre se manter conectada. Logo, diante da facilidade das trocas de informações no mundo contemporâneo virtual, o ambiente criptografado apareceu juntamente com a criação da internet e, por ser uma rede restrita, acabou atraindo grupos criminosos, que migraram para a camada oculta criptografada da rede de comunicação virtual. O intuito inicial da plataforma criptografada era manter em anônimo os usuários que buscavam a liberdade e a privacidade, sendo impossível que fosse revelada sua identidade ou conteúdo acessado. Com essa tecnologia no mercado, criminosos criaram o submundo digital, visando a permissão para a disseminação de conteúdo sem censura ou rastreamento através de fóruns e páginas indexados apenas no submundo da internet (*deep web dark web)*, os quais não são encontrados por meio dos mecanismos de pesquisa padrão. Com o surgimento dessa realidade virtual, as organizações criminosas se especializaram nas práticas de crimes dentro dos ambientes virtuais criptografados ocultos, tais como, lavagem de dinheiro, tráfico de drogas, pornografia infantil, estelionatos e etc. Para a realização da pesquisa, foi realizado um estudo sobre o funcionamento do mundo criminoso escondido nas redes de computadores, internet em uma escala global. Bem como os aumento de ataques utilizando o espaço virtual, a utilização de proteção criptografada por cibercriminosos para ocultação das práticas de crimes virtuais, a importância das autoridades investirem em cyber segurança e a ausência de norma regulamentadora para inibir essas práticas delituosas.

PALAVRAS-CHAVE: Deep Web, Crime Organizado, Crimes Cibernéticos, Investigação.

1 INTRODUÇÃO

Atualmente, com os constantes avanços da tecnologia mundial, a acessibilidade de *smartphones* modernos com acesso à internet tem possibilitado uma vida cotidiana mais ágil. Os índices de pessoas conectadas aumentam diariamente, se tornando uma ferramenta essencial para a vida das pessoas. Seria, sim, possível viver sem acesso a tecnologia nos tempos atuais, o fato é que a troca de informações em tempo real vem gerando uma dependência digital a nível global.

[1]Graduanda do 8º Semestre do curso de Direito do Centro Universitário FAG, vstferreira@minha.fag.edu.br.
[2]Docente do curso de Direito do Centro Universitário FAG, alexfadel@fag.edu.br.

A definição de internet é bastante abrangente, dado que conhecemos apenas uma parte de um mundo subterrâneo pouco conhecido pela sociedade, mas muito utilizado por criminosos. O submundo cibernético se divide em duas camadas, que são denominados *DEEP WEB* (parte profunda) e *DARK WEB* (parte escura), sendo a *deep web* composta por conteúdos não com buscas por meio de artigos científicos nas bases de dados: SciELO, Google Acadêmico, Revistas Tribunais e periódicos nacionais, por meio dos descritores: *deep web* e *dark web*, investigação e infiltração na *deep web*. O critério de exclusão e inclusão dos artigos foi estabelecido pela leitura dos resumos, títulos e verificação da relevância para o trabalho.

2 O MUNDO OCULTO DA *DEEP WEB E DARK WEB*

Primeiramente, no que tange a estruturação por inteiro do ambiente virtual, esta pode ser comparada como a forma de um iceberg. Tendo como sua superfície a primeira camada, na qual são indexados os conteúdos que podem ser acessados por todos os usuários.

Em sua segunda camada profunda encontra-se a *Deep Web*, pouco conhecida pela sociedade, pois seu acesso não se dá pelos mecanismos de pesquisas popularmente utilizados pelos usuários da internet (Google Chrome e o Firefox), sendo possível apenas através de um *software* específico, criado pelo Laboratório de Pesquisa Naval dos Estados Unidos, com o objetivo de proteger a comunicação do serviço de inteligência dos militares norte-americanos infiltrados em missões secretas, o *The Onion Routing (*conhecido por TOR, sigla em inglês), ou por navegador "cebola", que permite a navegação anônima utilizando a criptografia em camada, de onde vem a origem do nome.

Neste ambiente oculto não se encontra somente conteúdos de origem criminosa, mas também todos os conteúdos não indexados na camada superficial, sendo possível ter acesso a músicas e filmes raros, livros, fóruns, blogs e páginas que permitem trocas de informações entre os usuários, bem como artigos de pesquisas acadêmicas.

Considerado um meio de navegação seguro e utilizado em diversos países, que limitam a sociedade ao acesso de informação, é sempre recomendado o uso de VPN para proteção de ataques de *hackers*, que utilizam dessa plataforma com intuído de acessar os dados pessoais de quem entra na *deep web* sem proteção.

Por fim, a camada obscura se destina a *Dark Web*, que hospeda todo o conteúdo ruim e perverso, tais como o tráfico de drogas, a pedofilia infantil, os assassinos de aluguel, os terroristas e muitas outras práticas de crimes ilegais.

Para ter acesso a essa parte profunda da internet são necessários programas criptográfics complexos e *softwares* específicos, onde apenas quem possui o conhecimento avançado consegue ter acesso aos fóruns, comunidades e blogs restritos, com conteúdo criminoso, por exemplo para a compra e venda de armas, drogas, mercado clandestino de órgãos, e muitas

práticas de crimes deliberadas. Dentro do mundo perverso da internet, as famosas criptomoeda contribuíram para o avanço das transações financeiras, por se tratar de um método de pagamento criptografada.

A primeira vez que o termo *Deep Web* apareceu foi na pesquisa de Michael K. Bergman, que detalhou a dimensão do mundo oculto pouco conhecido:

> A *Deep Web* é cerca de 550 vezes maior do que a Camada Superficial da internet, com, em média, cerca de três vezes mais alta qualidade com base em nossos métodos de pontuação de documentos em uma base por documento. Em uma base absoluta, a qualidade total da *Deep Web* excede a da *Surface Web* por milhares de vezes. O número total de sites na *Deep Web* provavelmente excede 200.000 hoje e está crescendo rapidamente. O conteúdo na *Deep Web* tem significado e importância para cada buscador e mercado de informações. Mais de 95% das informações da *Deep Web* estão acessíveis sem restrição. A *Deep Web* também parece ser o componente de informação que cresce mais rapidamente na Web (BERGMAN, 2001). (Tradução livre.)

Neste contexto, é de suma importância ressaltar os delitos que podem ser encontrados nesta camada oculta. A respeito deste assunto, no ano de 2015, o especialista em investigação de crimes cibernéticos Leonardo Andrade trouxe em seu artigo as seguintes informações sobre este ambiente:

> Na Deep Web encontra-se de tudo. É possível, por exemplo, contratar assassinos de aluguel, comprar cartões de créditos roubados e/ou furtados, é onde se abrigam os maiores exploradores de pornografia infantil, sites de venda de órgãos humanos, armas químicas e de uso exclusivo das forças armadas, com destaque para o comércio de drogas que é altamente estruturado, difundido e rentável, grupos terroristas articulam-se nos fóruns secretos, grupos que discutem técnicas para matar pessoas por meio de práticas satânicas e dos mais variados tipos de parafilias (ANDRADE, 2015) p. 2.

As profundezas da internet abrigam diversos criminosos, que se esconde atras de computadores e por diversas camadas de criptografias, utilizada com o intuito de mascarar sua localização real do usuário. Com a ausência de ferramentas especificas pra interversão no mundo obscuro e norma regulamentados eficazes, criminosos se aproveitam disso, atuando livremente nos mais diversos crimes possíveis. Leonardo Andrade em seu artigo, discorre sobre:

> A situação agrava-se quando os cybercrimes são oriundos da *Deep Web*, pois, estes são tão sofisticados que sequer deixam rastros. O submundo da internet serve como um *bunker* para o criminoso digital que se aproveita das fragilidades e lacunas das leis, da ausência de fronteiras e das tecnologias disponíveis para manterem-se nas práticas delitivas. (ANDRADE, 2015) p.1

Não obstante, Silvana Drumond Monteiro e Marcos Vinicius Fidencio, detalham um pouco sobre o mundo invisível da Dark Web:

> A Dark Web ilustra bem a tensão entre a privacidade e a publicidade; a liberdade de expressão e até valores maniqueísta do bem e do mal, arquétipos humanos

> ressignificados ou virtualizados no ciberespaço. Embora o Freenet tenha sido pensado para uma Dark Net, ou seja, rede para compartilhamento de conteúdos e arquivos livres na Web (Biddle et al., 2002) seu uso tem sido feito, em grande parte, por criminosos, para a pedofilia, tráfico e satanismos (MONTEIRO, 2013) p.10.

No entanto, somente no ano de 2011 é que a *Dark Web* ficou conhecida pelo público, com o seguimento da plataforma denominada "*Silk Road" (rota da seda)* que estava localizada dentro da *deep web*, seu nome era uma referência as estradas que ligavam o comercio de mercadorias entre a Europa e Asia no século IX.

A plataforma foi criada e administrada pelo físico e pesquisador americano Ross William Ulbricht, que por muito tempo utilizou o pseudônimo de *Dread Pirate Roberts*, personagem de um romance *The Princess Bride* (1973), ficando assim conhecido na plataforma.

O operador de mercado da *darknet* obteve um grande sucesso no mercado negro, por intermediar a compra e venda desses produtos de forma totalmente anônima de drogas *online*, medicamentos de uso restrito e até mesmo produtos legalizados, e possibilitando que os usuários recebessem esses produtos em sua residência, através dos serviços de correspondências.

O caso de Ross Ulbricht teve uma grande repercussão na mídia americana, devido ao mercado ter se tornado viral nas redes, chamando também para si a atenção do FBI, que passou a investigar a plataforma no submundo digital.

Após meses de investigação, o departamento federal de investigação americano obteve uma informação dentro de um fórum contido no site, que anunciava uma possível vaga de emprego, juntamente com o endereço de e-mail do pesquisador, e através disso conseguiram efetuar a sua ligação com o administrador da plataforma Dread Pirate Roberts.

O trabalho dos investigadores possibilitou a localização de Ross Ulbricht, que foi preso e condenado a prisão perpétua no ano de 2015, por lavagem de dinheiro, invasão de computadores e facilitação para o tráfico de drogas.

2.1 A ATUAÇÃO DAS ORGANIZAÇÕES CRIMINOSAS NOS SUBMUNDOS DA INTERNET

A atuação dos cibercriminosos no mundo oculto da rede se divide em diversos delitos, sendo mais constantes os crimes de estelionato, divulgação e vendas de dados pessoais e pornografia infantil.

A ausência de limites e filtros juntamente com a camada de criptografias no submundo virtual contribuem para que criminosos tenham livre acesso a fóruns com os mais variados tipos de conteúdo criminosos inimagináveis que variam desde segredos de estado até as práticas de crimes de incitação de terrorismo, racismo, suicídio e discursos de ódios.

> [...] um dos pontos desfavoráveis desse universo é fato de que em grande parte da Deep Web encontram-se conteúdos ilegais. Diversos grupos beneficiam-se do anonimato para compartilhar conteúdo criminoso, carregando o espaço com páginas de pedofilia contendo imagens e vídeos explícitos, páginas de necrofilia, anúncios de assassinos de aluguel e suas tabelas de preços que variam de acordo com a importância social da vítima, zoonecrofilia, fóruns de canibalismo, além de uma espécie de Mercado Livre onde se pode encontrar desde drogas até armas e órgãos.

Para Assunção (2018), as espécies de crimes cibernéticos ou crimes virtuais referem-se a:

> Crimes de ódio em geral (contra a honra, sentimento religioso, bullyng), crimes de invasão de privacidade e intimidade (que pode ou não incorrer em uma nova conduta lesiva contra a honra), crimes de estelionato, crimes de pedofilia, entre outros. (ASSUNÇÃO, 2018, p. 11).

Para se ter acesso a determinados conteúdos restritos é necessário que os usuários saibam o domínio especifico o qual querem acessar. Contudo, é possível verificar a localização de sites e fóruns de trocas de informações através de mecanismo de busca como o *Torch*, informação contida na pesquisa de KOHN (2013).

> [...] um dos buscadores da Deep Web é o Torch. Com a ajuda deste mecanismo de busca é possível encontrar serviços de mensagens instantâneas e bibliotecas com livros raros sobre religião, psicologia e outros assuntos [...]". Além de acervos das mais variadas mídias, contudo, todos sem procedência. Por este motivo ressalta-se a necessidade de ter muito cuidado e atenção redobrada com determinados links listados nos resultados de busca (KOHN, 2013).

2.2 AS PRINCIPAIS DIFICULDADES ENCONTRADAS PELAS AUTORIDADES NA INVESTIGAÇÃO NA DEEP WEB

Até determinado tempo acreditava-se que os crimes praticados dentro da *deep web* eram impossíveis de serem solucionados, por conta da preservação do anonimado na navegação através de criptografia, o que sempre complicou a identificação de criminosos.

O tempo que demanda em uma investigação que necessita se efetuar a quebra de determinada criptografia é superior ao tempo que conteúdos são compartilhados nesta rede TOR, essas quebras de proteções são as maiores dificuldades enfrentadas pelas autoridades atualmente.

Porém no que se refere a possibilidade de investigação dos crimes nos ambientes virtuais, nos anos de 2012, 2014 e 2016 a Polícia Federal (PF), realizou duas operações em conjunto com o Ministério Público (MP) e a Interpol. A primeira, denominada *DirtyNet* e a segunda, denominada *DarkNe*t, com o intuito de desarticular uma quadrilha que se utilizava desse mundo obscuro, para a disseminação de pornografia infantil, em grupos restritos da deep web denominado Gigatribe.

No ano de 2017 a Policia Federal realizou a primeira fase da Operação *DarkNe*t, visando o combate à pornografia infantil. Policiais conseguiram rastrear o ambiente conhecido como *Deep Web*, com o uso de técnicas de infiltração policial, ambiente esse que era considerado um meio seguro para que usuários da internet compartilhassem anonimamente conteúdos perversos.

Nessa oportunidade os policiais conseguiram adentrar nesse mundo invisível, identificando mais de 90 pessoas que disseminavam a pornografia infantil, conforme informado através do site da Polícia Federal.

2.3 A CARÊNCIA DO ORDENAMENTO JURÍDICO

A respeito da ausência de formas punitivas específicas aos crimes virtuais, o Superior Tribunal de Justiça (2008) publicou um informativo eletrônico:

> Na ausência de uma legislação específica para crimes eletrônicos, os tribunais brasileiros estão enfrentando e punindo internautas, *crakers* e *hackers* que utilizam a rede mundial de computadores como instrumento para a prática de crimes. Grande parte dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, como a distribuição de vírus eletrônico, cavalos-de-tróia e *worm* (verme, em português).

Já o Ministro do Superior Tribunal de Justiça (STJ), Raul Araújo, enfatizou ao rebater as críticas acerca da regulamentação da web:

> A internet não é um universo sem lei. Os julgados do STJ retratam o cenário atual no Brasil ao mostrar que a internet é um espaço de liberdade, muito valioso para a busca de informações e o contato entre as pessoas, mas também de responsabilidade", explica o ministro Raul Araújo. "O Judiciário está atento ao direito das pessoas que têm a sua imagem violada. E os agressores, que imaginam estar encobertos pelo anonimato, serão devidamente responsabilizados por suas condutas.

Todavia, diante da perspectiva da Lei nº 12.737/2012, que ficou conhecida por Lei da Carolina Dieckmann, a mesma demostra-se insuficiente ao se tratar de crimes cibernéticos, visto que não tipifica condutas criminosos praticadas na *Deep Web*.

Dessa forma, demostra-se a necessidade da ampla discussão social a respeito desse tema pouco conhecido, pois nem tudo está apenas na superfície da internet e a ausência de normas que tipificam a prática criminosa na *deep web* merece ser estabelecida, visando a proteção do direito alheio.

3 CONSIDERAÇÕES FINAIS

O presente trabalho foi realizado mediante revisões bibliográficas, o qual buscou observar a expansão tecnológica e o comportamento das organizações criminosas no submundo da internet, com enfoque nos desafios de investigação pelas autoridades.

Ao longo de toda a pesquisa levantou-se um grande questionamento, de até que ponto a liberdade na rede oculta tende a chegar. E, analisando dados contidos em diversos artigos, nota-se que criminosos agem livremente dentro das plataformas ocultas na camada profunda da internet.

Diante da impossibilidade de monitoramento e dos mecanismos de controle oficiais, da ausência de investimento em tecnologia para investigações digitais e normas que tipificam a conduta na *deep web*, a investigação de crimes dentro desse mundo tem se tornado uma das maiores barreiras na atuação das autoridades.

No entanto, por se tratar de uma área em constante evolução, as autoridades públicas têm se unido, buscando a integração de informações e métodos de investigação e deflagrando operações conjuntas para se infiltrarem entre as organizações criminosas virtuais e, assim, se tornar possível a identificação desses cibercriminosos, de modo a se tornar possível a prisão dos mesmo.

REFERÊNCIAS

ALVES, M. H. dos S**. A evolução dos crimes cibernéticos e ao acompanhamento das leisespecíficas no Brasil**. Publicado em 2018. Disponível em: < https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-o-acompanhamento- das-leis-especificas-no-brasil#:~:text=punir%20os%20infratores.-,Percebe%2Dse%20que%20a%20norma%20jur%C3%ADdica%20brasileira%20n%C3%A3o%20acompanhou%20a,ao%20estado%20punir%20os%20infratores.> Acesso em 15 abr. 2021 ANDRADE, Leonardo. Cybercrimes na deep web**: as dificuldades de determinação de autoria nos crimes virtuais.** Jus.com.br, 2015. Disponível em: https://jus.com.br/artigos/39754/cybercrimes-na-deep-web-as-dificuldades-juridicas-de-determinacao-de-autoria-nos-crimes-virtuais. Acesso em: 19/11/2021.

BERGMAN, Michael K. ***The Deep Web: Surfacing Hidden Value***. 2001. Disponível em:<White Paper: The Deep Web: Surfacing Hidden Value (umich.edu)> . Acesso em: 19 nov. 20221.

EMÍDIO LUCENA, Fabiano; PALITOT BRAGA, Romulo Rhemo. **O fenômeno da lavagem de dinheiro e o tráfico de drogas na deep web: Avanço da criminalidade virtual.** In: Revista Brasileira de Ciências Criminais. São Paulo, 2016.w\a.

MONTEIRO, Silvana Drumond; FIDENCIO, Marcos Vinicius**. As dobras semióticas do ciberespaço: da web visível à invisível**. TransInformação, abr. 2013. Disponível em: <https://www.scielo.br/j/tinf/a/Pk5r9yxsgkbyRWctn6Rd4GH/?format=pdf&lang=pt> Acesso em: 19 nov. 2021.

POLICIA FEDERAL. **Balanço Final da Operação DirtyNet**. jun. 2012. Disponível em:. Disponível em: <http://www.pf.gov.br/agencia/noticias/2012/junho/balanco-final-da-operacao-dirty-net/> A Acesso em: 18 set. 2021.

POLICIA FEDERAL. **Combate a disseminação de pornografia infantil pela deep web no Rio Grande do Sul**. out. 2014. Disponível em: <http://www.pf.gov.br/agencia/noticias/2014/10/pf-combate-a-disseminacao- de-pornografia-infantil-pela-deep-web-no-rs/> Acesso em: 18 set. 2021.

POLICIA FEDERAL. **Combate crime de pornografia infantil na deep web**. nov. 2016. Disponível em: <http://www.pf.gov.br/agencia/noticias/2016/11/pf-combate-crime-de-pornografia-infantil-na-deep-web> Acesso em: 18 set. 2021.

ROCHA, A. A. **Cibercriminalidade os crimes cibernéticos e os limites da liberdade de expressão na internet**. Curso de Direito da Universidade Tiradentes – UNIT. Garça-SP, 2017. Disponível em: https://www.faef.br/userfiles/files/23%20-%20cibercriminalidade%20e%20os%20limites%20da%20liberdade%20de%20expressao%20na%20internet.pdf> Acesso em 18 set. 2021.