ISSN 2447-1097

Direito & TI – Porto Alegre / RS www.direitoeti.com.br

A *DEEP WEB* E A RELAÇÃO COM A CRIMINALIDADE NA INTERNET

Daniela Cristina Borges[1]
Liane Pioner Sartori[2]
Mauricio Sebastião de Barros[3]

RESUMO

Atualmente, o uso da Internet faz parte do cotidiano de grande parte da população, tanto no Brasil como no mundo e, de forma geral, tornou-se uma tecnologia imprescindível para as relações sociais e empresariais. Ocorre que, simultaneamente com o benefício dos serviços e funcionalidades conexas à Internet, surgiram os chamados crimes virtuais. Não são poucos os casos de vítimas (pessoas e empresas) que acabam lesadas com a má intenção de alguns usuários da rede mundial de computadores. Nesse contexto, surge a *Deep Web* (Internet profunda em uma tradução livre), que é uma "área" ainda pouco explorada pelo grande público em relação à Internet, o que facilita o cometimento de crimes, ante o fato de os endereços e acessos serem mais difíceis de rastrear. Na mesma medida em que há perigo em determinadas ações na Internet convencional, a *Deep Web* apresenta ainda mais riscos, o que exige cautela dos usuários quando do acesso e uso.

Palavras-chave: Crimes Virtuais; *Deep Web*; Internet; Tecnologia da Informação.

INTRODUÇÃO

A Internet tornou-se indispensável para grande parte da população mundial. A partir da rede, é possível pesquisar, fazer transações financeiras e comerciais, trabalhar de forma remota (a distância), acessar as redes sociais, trocar arquivos, dentre tantas outras possibilidades de utilização. Todavia, criminosos têm utilizado esta tecnologia para realizar práticas delituosas, com o intuito de obter, para si ou para outrem, vantagens em proveito de outros internautas.

Um dos grandes problemas em relação aos delitos praticados via Internet é ainda a grande sensação de inpunidade, uma vez que a criminalidade avançou mais rapidamente do que a legislação e do que as técnicas para identificar os autores dos crimes. Como efeito, os crimes virtuais vêm se tornando corriqueiros no Brasil e no mundo, de forma geral e, infelizmente, a dificuldade do poder legislativo em tipificar essas modalidades de crimes vem criando um clima de "terra sem lei" na Internet, pois os criminosos sabem que sua identificação é difícil. Aliás, cabe lembrar que, no Direito Penal brasileiro, lei não se interpreta: ou a conduta é típica ou não existe crime. É nesse contexto que

[1] Acadêmica de Gestão da Tecnologia da Informação. E-mail: dani.borges@msn.com.
[2] Mestre em Direito, Policial Civil. E-mail: liane.sartori@gmail.com.
[3] Mestre em Educação, Perito Forense Computacional. E-mail: mauriciobarros@ftec.com.br.

se insere a *Deep Web*, também conhecida como "Internet profunda". *A Deep Web* representa todo o conteúdo online não indexado, no que se incluem dados bancários, códigos administrativos, bases de dados e outras segmentações para os governos, corporações, universidades, entre outros.

1 *DEEP WEB*

A *Deep Web* é o conjunto de conteúdos da internet não acessível diretamente por sites de busca. Isso inclui, por exemplo e em regra, documentos hospedados dentro de sites que exigem login e senha. Sua origem e sua proposta original são legítimas. Afinal, nem todo material deve ser acessado por qualquer usuário (pode ficar dentro de sites comuns, na forma de arquivos e dados baixáveis, ou escondidos em endereços excluídos propositadamente dos mecanismos de busca).

A Internet convencional, também conhecida como "*Surface Web*", é formada por computadores com conteúdos conectados entre si, através de uma rede de links espalhados pelo mundo. Na internet comum é possível localizar qualquer máquina desde que se conheça o endereço chamado IP (*Internet Protocol*), ou seja, o IP é um endereço único que cada computador ou servidor possui para ser acessado via Internet.

Para que não haja necessidade de decorar números (sequência de números), optou-se pelo uso de servidores de nomes (*Domain Name System*), máquinas que possuem uma lista com as correspondências entre o IP e um endereço nominal. Por exemplo, o site da Receita Federal está hospedado em um *Host* (servidor ou conjunto de servidores) com o IP "161.148.231.100", mas quem quer encontrar a página da Receita Federal não precisa digitar os números, bastando digitar o endereço "www.receita.fazenda.gov.br", que aponta para o referido IP. E, com base nestes endereços, os buscadores web acessam esses servidores de nomes e rastreiam detalhadamente todos os conteúdos com permissão para serem acessados.

Quanto ao seu tamanho, estudos estimam que a *Deep Web* seja 500 vezes maior que a *Surface Web*. Especula-se, também, que a parte convencional da Internet que os usuários acessam todos os dias compreende apenas 5% do todo. O uso da *Deep Web* é bastante variado, e é aqui que reside a polêmica. Por causa da privacidade, muitas pessoas e organizações usam essa rede para compartilhar e hospedar arquivos sigilosos e que não podem estar disponíveis na "Internet convencional". O exército, as forças policiais, jornalistas, universidades e até mesmo cidadãos comuns com algum conhecimento de Internet são exemplo de pessoas que recorrem à *Deep Web* para fins específicos[1].

Uma das formas mais comuns de acessar os conteúdos da *Deep Web* é com a utilização de um aplicativo específico, como o TOR (*The Onion Router*), que é uma rede de túneis virtuais que dificulta e faz um mascaramento da identificação dos equipamentos ao acessarem determinado conteúdo. O TOR dificulta o rastreamento, mas não garante a inviolabilidade dos dados nem a identidade da máquina (computador ou servidor) porque não é criptografado.

Além disso, uma análise de tráfego seria capaz de revelar muitas informações sobre o que uma pessoa faz na *Deep Web*, uma vez que são monitoráveis a origem, o destino, o tamanho e o tempo dos dados transmitidos, e assim poderia inferir quem está interagindo com quem. Mas o TOR não é a única forma de acesso à *Deep Web*, havendo outros aplicativos como o *Morphmix*, *Mixminion*, *Mixmaster*, *AntsP2P*, *Haystack*, entre outros.

Ao contrário do que muitos podem imaginar, acessar a *Deep Web* não é ilegal. Motivados pela privacidade que o local pode proporcionar, várias pessoas recorrem à "internet invisível" para tratar de assuntos sigilosos e compartilhar arquivos que jamais poderiam "ver à luz do dia". No entanto, a condição de anonimato (o que é vedado pela Constituição Federal[i]) dessa gigantesca parte da Internet também acaba levando ao surgimento de uma série de atividades ilegais, muitas das quais os órgãos competentes ainda têm muita dificuldade em tratar.

2 A CRIMINALIDADE NA INTERNET

Neste contexto, verifica-se que o combate à criminalidade na Internet encontra diversos problemas relacionados não somente às lacunas jurídicas, mas também aos reflexos que podem causar na restrição à liberdade de expressão e ao acelerado desenvolvimento tecnológico. O anonimato permitido pela estrutura virtual, que caracteriza a *Deep Web*, dificulta a identificação do autor. Outrossim, a identificação e a localização do criminoso é insuficiente para a lavratura do auto de prisão em flagrante do mesmo, haja vista que tais dados são obtidos, geralmente, quando já transcorrido lapso temporal suficiente para não configurar a prisão em flagrante[ii].

O amplo acesso da população à Internet, em paradoxo à falta de conscientização da importância da prevenção através de medidas de segurança, reflete outra fragilidade da Internet, tanto que muitas pessoas fazem uso da rede sem se preocupar com o perigo de invasão ao computador, sem a utilização de softwares de segurança, sem verificar a credibilidade de uma empresa que oferece serviços online no momento de efetuar um pagamento ou de inserir dados pessoais.

Demais disso, a Lei nº 12.737, sancionada em 2012, conhecida como a "Lei dos Crimes Cibernéticos", mostra-se, por ora, insuficiente para repreender os crimes dessa natureza, por não tipificar todas as condutas possíveis no universo da *Deep Web*. A falta de limites estabelecidos na jurisdição acerca do tema gera problemas relacionados à própria soberania nacional, nos casos em que mais de um país esteja envolvido, dada a falta de fronteiras do mundo virtual. Nem mesmo a jurisdição pode ser definida em casos envolvendo crimes cibernéticos, dado o princípio da territorialidade adotado pela legislação brasileira[iii].

Diante disso, a determinação dos lugares em que o crime foi executado e gerou resultados, assim como a definição da materialidade, da autoria e da culpabilidade, tornam-se barreiras aos procedimentos investigatórios, ao passo que muitos criminosos virtuais são estudiosos e estão constantemente buscando novos horizontes e oportunidades para aplicar seus conhecimentos.

Por outro lado, a justiça brasileira, trabalha no intuito de manter a liberdade e a legalidade do uso da Internet de forma geral, conforme declaração do Ministro Raul Araújo, do Superior Tribunal de Justiça (STJ):

> 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.

No âmbito internacional, tem-se como marco a Convenção sobre o Cibercrime (Convenção de Budapeste), tratado internacional de direito penal e direito processual penal firmado no âmbito do Conselho da Europa para definir (de forma harmônica) como os crimes praticados por meio da Internet e as formas de persecução são tratados, basicamente as violações de direito autoral, fraudes relacionadas a computador, pornografia infantil e violações de segurança de redes. A Convenção foi adotada pelo Comitê de Ministros do Conselho da Europa na Sessão 109 de novembro de 2001 e entrou em vigor em 01 de julho de 2004. Porém, o Brasil não a ratificou.

CONSIDERAÇÕES FINAIS

Ante todo o exposto, tem-se que a utilização da Internet cresce em proporção similar em que aumenta a criminalidade tecnológica (dita virtual), fazendo com que cada vez mais a sociedade se preocupe com a situação.

Dessa forma, a fim de evitar que mais pessoas e organizações sejam vítimas de crimes cibernéticos, mostram-se imperiosos tanto o avanço legislativo no que tange à matéria, como o investimento em tecnologia e capacitação pessoal por parte dos órgãos competentes na elucidação de delitos e de punição dos criminosos.

Tem-se claro que o acesso a *Deep Web* não é ilegal, mas o anonimato permitido por ela facilita a utilização dessa parte da Internet para o cometimento de crimes, situação que não pode ser tolerada pelos órgãos públicos, tampouco enfrentada de forma assídua pela sociedade, sob pena de sermos vítima da criminosa realidade virtual.

REFERÊNCIAS

MARTINELLI, João Paulo Orsini. **Aspectos relevantes da criminalidade na internet**. Disponível em: <http://jus.com.br/artigos/1829/aspectos-relevantes-da-criminalidade-na-internet>. Acesso em: 16 out. 2015.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963> Acesso em 16 out. 2015.

PEDROSA, Leyberson. **Entenda o que é Deep Web e saiba os riscos de navegação**. Disponível em: <http://www.ebc.com.br/tecnologia/2013/08/deep-web-riscos-e-usos-possiveis>. Acesso em: 19 set. 2015.

ROHR, Altieres. Acesso a sites anônimos. Disponível em: <http://g1.globo.com/tecnologia/noticia/2015/06/acesso-sites-anonimos-da-deep-web-e-facil-de-monitorar-diz-estudo.html>. **G1 Tecnologia**. Acesso em: 19 set. 2015.

SAIBA NA WEB. ***Deep web***: O que são os bitcoins. Disponível em: <http://www.saibanaweb.com/2013/04/bitcoin.html>. Acesso em: 16 out. 2015.

[i] Constituição Federal. Art. 5º (...) IV – É livre a manifestação do pensamento, sendo vedado o anonimato.

[ii] Nos termos do artigo 302 do Código de Processo Penal, considera-se em flagrante delito quem está cometendo a infração penal; quem acabou de cometê-la; quem é perseguido, logo após, pela autoridade, pelo ofendido ou por qualquer pessoa, em situação que faça presumir ser o autor da infração; ou quem é encontrado, logo depois, instrumentos, armas objetos ou papéis que façam presumir ser ele autor da infração.

[iii] Em conformidade com o artigo 5º do Código Penal, "Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido em território nacional".